

(51) 国際特許分類7

H04L 9/08, 9/32, 12/28, H04H 1/00,  
H04N 7/167

A1

(11) 国際公開番号

WO00/62475

(43) 国際公開日

2000年10月19日(19.10.00)

(21) 国際出願番号

PCT/JP00/02353

(22) 国際出願日

2000年4月11日(11.04.00)

(30) 優先権データ

特願平11/105966

1999年4月13日(13.04.99)

JP

特願平11/143988

1999年5月24日(24.05.99)

JP

(71) 出願人 (米国を除くすべての指定国について)

ソニー株式会社(SONY CORPORATION)[JP/JP]

〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)

(72) 発明者 ; および

(75) 発明者 / 出願人 (米国についてのみ)

浅野智之(ASANO, Tomoyuki)[JP/JP]

大澤義知(OSAWA, Yoshitoimo)[JP/JP]

〒141-0001 東京都品川区北品川6丁目7番35号

ソニー株式会社内 Tokyo, (JP)

(74) 代理人

小池 晃, 外(KOIKE, Akira et al.)

〒105-0001 東京都港区虎ノ門二丁目6番4号

第11森ビル Tokyo, (JP)

(81) 指定国 JP, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)

添付公開書類

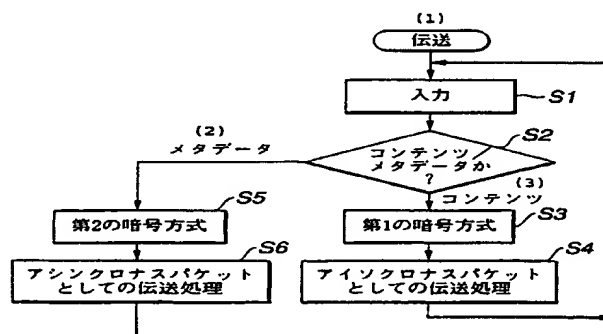
国際調査報告書

(54)Title: INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING METHOD, AND INFORMATION PROCESSING DEVICE

(54)発明の名称 情報処理システム、情報処理方法及び情報処理装置

## (57) Abstract

Protocol for mutual authentication and for sharing a plurality of encryption keys is practiced between a CPU (12) on a data transmitter (10) side and a CPU (22) on a data receiver (20) side prior to data transmission. The data transmitter (10) encrypts data which requires assurance of a transmission band with a first encryption key by the CPU (12) and transmits it through an input/output interface (16) in a first transmission mode. The data transmitter (10) further encrypts related data concerning the above mentioned data with a second encryption key through the input/output interface (16) in a second transmission mode. The data receiver (20) decrypts the data which requires the assurance of the transmission band and is received through an input/output interface (24) in the first transmission mode with the first code key and decrypts the related data which are received through the input/output interface (24) in the second transmission mode with the second code key.



S1...INPUT  
S2...CONTENTS OR META-DATA?  
S3...1ST ENCRYPTION METHOD  
S4...TRANSMIT DATA AS ISOCRONOUS PACKET  
S5...2ND ENCRYPTION METHOD  
S6...TRANSMIT DATA AS ASYNCHRONOUS PACKET  
(1)...TRANSMISSION  
(2)...META-DATA  
(3)...CONTENTS

データ送信装置 10 側の CPU 12 とデータ受信装置 20 側の CPU 22 との間で、データ伝送に先立って、相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する。データ送信装置 10 は、伝送帯域の保証が必要なデータを上記 CPU 12 により第 1 の暗号鍵で暗号化して第 1 の伝送モードで入出力インターフェース 16 を介して送信し、上記データに関する関連データを第 2 の暗号鍵で暗号化して第 2 の伝送モードで上記入出力インターフェース 16 を介して送信し、上記データ受信装置 20 は、上記 CPU 22 により、入出力インターフェース 24 を介して第 1 の伝送モードで受信される上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で復号し、上記入出力インターフェース 24 を介して第 2 の伝送モードで受信される上記関連データを第 2 の暗号鍵で復号する。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スーダン
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LK	スリ・ランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボスニア・ヘルツェゴビナ	GB	英国	LU	ルクセンブルグ	SN	セネガル
BB	バルバドス	GD	グレナダ	LV	ラトヴィア	SZ	スワジランド
BE	ベルギー	GE	グルジア	MA	モロッコ	TD	チャード
BF	ブルキナ・ファソ	GH	ガーナ	MC	モナコ	TG	トーゴ
BG	ブルガリア	GM	ガンビア	MD	モルドヴァ	TJ	タジキスタン
BJ	ベナン	GN	ギニア	MG	マダガスカル	TM	トルクメニスタン
BR	ブラジル	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサウ		共和国	TT	トリニダード・トバゴ
CA	カナダ	HR	クロアチア	ML	マリ	TZ	タンザニア
CF	中央アフリカ	HU	ハンガリー	MN	モンゴル	UA	ウクライナ
CG	コンゴ	ID	インドネシア	MR	モリタニア	UG	ウガンダ
CH	スイス	IE	アイルランド	MW	マラウイ	US	米国
CI	コートジボアール	IL	イスラエル	MX	メキシコ	UZ	ウズベキスタン
CM	カメルーン	IN	インド	MZ	モザンビーク	VN	ヴェトナム
CN	中国	IS	アイスランド	NE	ニジェール	YU	ユーゴスラヴィア
CR	コスタ・リカ	IT	イタリア	NL	オランダ	ZA	南アフリカ共和国
CU	キューバ	JP	日本	NO	ノルウェー	ZW	ジンバブエ
CY	キプロス	KE	ケニア	NZ	ニュージーランド		
CZ	チェッコ	KG	キルギスタン	PL	ポーランド		
DE	ドイツ	KP	北朝鮮	PT	ポルトガル		
DK	デンマーク	KR	韓国	RO	ルーマニア		

## 明細書

### 情報処理システム、情報処理方法及び情報処理装置

#### 技術分野

本発明は、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースを介してデータの伝送を行う情報処理システム、情報処理方法及び情報処理装置に関する。

#### 背景技術

近年、例えば家庭内において、複数のＡＶ機器をデジタルインターフェースを介して接続し、音楽情報や映像情報などのデジタルデータを伝送したり記録したりするようにしたシステムが普及しつつある。

例えば、デジタルバスであるＩＥＥＥ(The International of Electrical and Electronics Engineers, Inc.) 1394ハイ・パフォーマンス・シリアル・バス(以下、単にＩＥＥＥ1394シリアルバスという)のインターフェースを持つビデオカメラやＤＶＤプレーヤなどの機器では、データを高品質で記録することが可能であ

ることから、著作権のあるデータが不正にコピーされてしまうのを防止する必要がある。

例えば、光磁気ディスク装置に映画情報を記録することが許可されているか否かを表す情報を記憶しておき、この情報を利用して、その光磁気ディスク装置が正当な装置すなわち著作権者からのライセンスを受けた装置であるか否かを認証するようにし、正当な装置として認証された光磁気ディスク装置のみに映画情報の記録を許可するようにすることが行われる。このような場合、映画情報を伝送する側の装置（以下、このような装置をソース(source)という）と、伝送を受けた装置（以下、このような装置をシンク(sink)という）との間で、相手側の装置が適正な装置であるか否かを認証する必要がある。

このようなシステムにおける著作権保護を目的として、様々な認証方式が提案されている。これらの認証方式に用いられる認証プロトコルには、暗号アルゴリズムが用いられることが多い。

ところで、音楽データを機器間で伝送する際には、例えば、音楽データの伝送途中に伝送が止まったり、伝送できるデータ量が極端に減ったりすると、受信側で音楽の再生に必要なデータが得られなくなり、音楽が途切れてしまうおそれがあるので、ある程度の帯域を確保した状態で音楽データを伝送する必要がある。

一方、音楽データそのものではないが、音楽データに関連した情報として、例えば歌詞やアーティストの写真などを伝送する場合には、音楽データそのものの伝送する場合に比べて、リアルタイム性を必要としないので、伝送帯域が確保されていない伝送方式を用いて伝送することが可能である。一般に、伝送帯域が確保されていない



伝送方式を用いる方が、伝送路全体の帯域を消費しないという点で望まれることが多い。

#### 発明の開示

そこで、本発明の目的は、上述の如き従来の問題点に鑑み、伝送帯域が確保された伝送方式と伝送帯域が確保されていない伝送方式の２種類の伝送方式を採用して、データを確実に伝送することができるようにした情報処理システム、情報処理方法、情報処理装置を提供することにある。

また、本発明の他の目的は、伝送帯域の保証が必要なデータと上記データに関する関連データを異なる暗号鍵により暗号化して安全に伝送することができるようにした情報処理システム、情報処理方法、情報処理装置を提供することにある。

さらに、本発明の他の目的は、送信側の情報処理装置と受信側の情報処理装置が互いの正当性を認証するとともに、暗号鍵を共有することができるようにした情報処理システム、情報処理方法、情報処理装置を提供することにある。

本発明に係る情報処理システムは、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝送モードで上記インターフェースを介して送信し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで上記インターフェースを介して送信する

送信制御手段とを備える第 1 の情報処理装置と、伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースと、上記インターフェースを介して第 1 の伝送モードで受信される上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で復号し、上記インターフェースを介して第 2 の伝送モードで受信される上記関連データを第 2 の暗号鍵で復号する受信制御手段とを備える第 2 の情報処理装置とを具備することを特徴とする。

また、本発明は、第 1 の情報処理装置と第 2 の情報処理装置との間で伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースを介してデータ伝送を行う情報処理方法であって、上記第 1 の情報処理装置から伝送帯域の保証が必要なデータを第 1 の暗号鍵で暗号化して第 1 の伝送モードで送信するとともに、上記データに関する関連データを第 2 の暗号鍵で暗号化して第 2 の伝送モードで送信し、上記第 2 の情報処理装置側で第 1 の伝送モードで受信される上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で復号し、第 2 の伝送モードで受信される上記関連データを第 2 の暗号鍵で復号することを特徴とする。

また、本発明に係る情報処理装置は、伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースと、上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で暗号化して第 1 の伝送モードで上記インターフェースを介して送信し、上記データに関する関連データを第 2 の暗号鍵で暗号化して第 2 の伝送モードで上記インターフェースを介して送信する送信制御手段とを備えることを特徴とする。

さらに、本発明に係る情報処理装置は、伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースと、上記インターフェースを介して第 1 の伝送モードで受信される上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で復号し、上記インターフェースを介して第 2 の伝送モードで受信される上記関連データを第 2 の暗号鍵で復号する受信制御手段とを備えることを特徴とする。

#### 図面の簡単な説明

図 1 は、本発明を適用した A V システムを含むデジタル衛星放送システムの全体構成をブロック図である。

図 2 は、上記デジタル衛星放送システムにおける地上局の構成を示すブロック図である。

図 3 は、上記地上局から送信されるデータを示す図である。

図 4 A ～図 4 H は、送信データの時分割多重化構造を示す説明図である。

図 5 は、本発明を適用したデータ伝送システムの構成を示すブロック図である。

図 6 は、I E E E 1 3 9 4 バスケーブルの構造を模式的に示す説明図である。

図 7 A ～図 7 C は、I E E E 1 3 9 4 における信号伝送形態を示す説明図である。

図 8 は、I E E E 1 3 9 4 における P a c k e t 送信の概要を示

す説明図である。

図 9 は、上記データ伝送システムにおけるデータ送信装置の要部構成を示すブロック図である。

図 10 は、上記データ送信装置の動作を示すフローチャートである。

図 11 は、上記データ伝送システムにおけるデータ伝送の手順を示すフローチャートである。

図 12 は、上記データ伝送システムにおけるデータ送信装置側の処理手順を示すフローチャートである。

図 13 は、上記データ伝送システムにおけるデータ受信装置側の処理手順を示すフローチャートである。

図 14 は、上記データ伝送システムにおけるデータ伝送の他の手順を示すフローチャートである。

図 15 は、上記データ伝送システムにおけるデータ送信装置側の他の処理手順を示すフローチャートである。

図 16 は、上記データ伝送システムにおけるデータ受信装置側の他の処理手順を示すフローチャートである。

#### 発明を実施するための最良の形態

以下、本発明を実施するための最良の形態について図面を参照しながら詳細に説明する。

本発明は、各種デジタル A V (Audio Visual) 機器やパーソナルコンピュータ装置等の電子機器を、例えば I E E E (Institute of El

ectrical Engineers) 1 3 9 4 バスを介して相互に接続することで、機器間でデータを送受信できるようにしたデータ伝送システム (A V システム) に適用される。この A V システムは、デジタル衛星放送を受信して、受信データをダウンロード可能な構成が採られるものである。

この A V システムを含むデジタル衛星放送システムの全体構成を図 1 に示してある。

この図 1 に示したデジタル衛星放送システムにおいて、デジタル衛星放送の地上局 1 0 1 には、テレビ番組素材サーバ 1 0 6 からのテレビ番組放送のための素材と、楽曲素材サーバ 1 0 7 からの楽曲データの素材と、音声付加情報サーバ 1 0 8 からの音声付加情報と、G U I (Graphical User Interface) データサーバ 1 0 9 からの G U I データとが送られる。

テレビ番組素材サーバ 1 0 6 は、通常の放送番組の素材を提供するサーバである。このテレビ番組素材サーバから送られてくる音楽放送の素材は、動画及び音声とされる。例えば、音楽放送番組であれば、上記テレビ番組素材サーバ 1 0 6 の動画及び音声の素材を利用して、例えば新曲のプロモーション用の動画及び音声が発送されたりすることになる。

楽曲素材サーバ 1 0 7 は、オーディオチャンネルを使用して、オーディオ番組を提供するサーバである。このオーディオ番組の素材は音声のみとなる。この楽曲素材サーバ 1 0 7 は、複数のオーディオチャンネルのオーディオ番組の素材を地上局 1 0 1 に伝送する。

各オーディオチャンネルの番組放送ではそれぞれ同一の楽曲が所定の単位時間繰返して放送される。各オーディオチャンネルは、

それぞれ、独立しており、その利用方法としては各種考えられる。例えば、1つのオーディオチャンネルでは最新の日本のポップスの数曲を或る一定時間繰り返し放送し、他のオーディオチャンネルでは最新の外国のポップスの数曲を或る一定時間繰り返し放送するというようにされる。

音声付加情報サーバ108は、楽曲素材サーバ107から出力される楽曲の演奏時間等を提供するサーバである。

GUIデータサーバ109は、ユーザが操作に用いるGUI画面を形成するための「GUIデータ」を提供する。例えば後述するような楽曲のダウンロードに関するGUI画面であれば、配信される楽曲のリストページや各楽曲の情報ページを形成するための画像データ、テキストデータ、アルバムジャケットの静止画を形成するためのデータなどを提供する。さらには、AVシステム103側にていわゆるEPG(Electrical Program Guide)といわれる番組表表示を行うのに利用されるEPGデータもここから提供される。

なお、「GUIデータ」としては、例えばMHEG(Multimedia Hypermedia Information Coding Experts Group)方式が採用される。MHEGとは、マルチメディア情報、手順、操作などのそれぞれと、その組合せをオブジェクトとして捉え、それらのオブジェクトを符号化した上で、タイトル(例えばGUI画面)として制作するためのシナリオ記述の国際標準である。また、このデジタル衛星放送システムではMHEG-5を採用するものとする。

地上局101は上記テレビ番組素材サーバ106、楽曲素材サーバ107、音声付加情報サーバ108及びGUIデータサーバ109から伝送された情報を多重化して送信する。

このデジタル衛星放送システムでは、テレビ番組素材サーバ 106 から伝送されたビデオデータは M P E G (Moving Picture Experts Group) 2 方式により圧縮符号化され、オーディオデータは M P E G 2 オーディオ方式により圧縮符号化される。また、楽曲素材サーバ 107 から伝送されたオーディオデータは、オーディオチャンネルごとに対応して、例えば M P E G 2 オーディオ方式と、A T R A C (Adaptive Transform Acoustic Coding) 方式の何れか一方の方式により圧縮符号化される。

また、これらのデータは多重化の際、キー情報サーバ 110 からのキー情報を利用して暗号化される。

地上局 101 からの信号は衛星 102 を介して各家庭の受信設備（以降、A V システムともいう）103 で受信される。衛星 102 には複数のトランスポンダが搭載されている。1 つのトランスポンダは例えば 30 M b p s の伝送能力を有している。各家庭の A V システム 103 は、パラボラアンテナ 111 に接続された I R D (Integrated Receiver Decoder) 112 と、この I R D 112 に接続されたモニタ装置 114 及び M D レコーダ／プレーヤ 1 とからなる。また、この A V システム 103 は、I R D 112 に対して操作を行うためのリモートコントローラ 64 と、M D レコーダ／プレーヤ 1 に対して操作を行うためのリモートコントローラ 32 を備えている。

この A V システム 103 では、パラボラアンテナ 111 で衛星 102 を介して放送されてきた信号が受信される。この受信信号がパラボラアンテナ 111 に取り付けられた L N B (Low Noise Block Down Converter) 115 で所定の周波数に変換され、I R D 112 に供給される。

I R D 1 1 2における概略的な動作としては、受信信号から所定のチャンネルの信号を選局し、その選局された信号から番組としてのビデオデータ及びオーディオデータの復調を行ってビデオ信号、オーディオ信号として出力する。また、I R D 1 1 2では、番組としてのデータと共に多重化されて送信されてくる、G U I データに基づいてG U I 画面としての出力も行う。このようなI R D 1 1 2の出力は、例えばモニタ装置 1 1 4 に対して供給される。これにより、モニタ装置 1 1 4 では、I R D 1 1 2 により受信選局した番組の画像表示及び音声出力が行われ、また、ユーザの操作に従ってG U I 画面を表示させることが可能となる。

M D レコーダ／プレーヤ 1 は、装填されたミニディスクに対するオーディオデータの記録及び再生が可能な記録再生装置である。また、このM D レコーダ／プレーヤ 1 は、オーディオデータ（楽曲データ）及びこれに付随して関連付けされたアルバムジャケット等の静止画像データ（ピクチャファイル）、歌詞やライナーノーツ等のテキストデータ（テキストファイル）をディスクに記録し、かつ、記録されたこれらのピクチャファイル及びテキストファイル等のデータをオーディオデータの再生時間に同期させて再生出力することができるものである。

なお、上記オーディオデータに付随したピクチャファイル及びテキストファイル等のデータについては、後述するM D レコーダ／プレーヤ 1 での扱いに従って、便宜上「A U X データ」ともいう。

ここで、このA V システム 1 0 3 において、I R D 1 1 2 及びM D レコーダ／プレーヤ 1 は、I E E E 1 3 9 4 バス 1 1 6 によって相互接続されているものとされる。



つまり、AVシステム103を構築しているIRD112及びMDレコーダ/プレーヤ1は、それぞれデータ伝送規格としてIEEE1394に対応したデータインターフェイスを備えている。

これによって、このAVシステムでは、IRD112にて受信された楽曲としてのオーディオデータ（ダウンロードデータ）を、ATRAC方式により圧縮処理が施されたままの状態ですべて直接取り込んで記録することができる。また、上記オーディオデータと共に送信側のサーバーから衛星にアップロードされるAUXデータを、上記衛星からIRD112を介してMDレコーダにダウンロードして記録することも可能とされている。

IRD112は、電話回線104を介して課金サーバ105と通信可能とされている。IRD112には、各種情報が記憶されるICカードが挿入されるようになっている。そして、例えば楽曲のオーディオデータのダウンロードが行われたとすると、これに関する履歴情報がICカードに記憶される。このICカードの情報は、電話回線104を介して所定の機会、タイミングで課金サーバ105に送られる。課金サーバ105は、この送られてきた履歴情報に従って金額を設定して課金処理を行い、ユーザに請求する。

これまでの説明から分かるように、本発明を適用したAVシステムを含むデジタル衛星放送システムでは、地上局101は、テレビ番組素材サーバ106からの音楽番組放送の素材となるビデオデータ及びオーディオデータと、楽曲素材サーバ107からのオーディオチャンネルの素材となるオーディオデータと、音声付加情報サーバ108からの音声データと、GUIデータサーバ109からのGUIデータとを多重化して送信している。

そして、各家庭のA Vシステム103でこの放送を受信すると、例えばモニタ装置114により、選局したチャンネルの番組を視聴することができる。また、番組のデータと共に送信されるG U I データを利用したG U I 画面として、E P G (Electrical Program Guide; 電子番組ガイド) 画面を表示させ、番組の検索等を行うことができる。また、例えば通常の番組放送以外の特定のサービス用のG U I 画面を利用して所要の操作を行うことで、放送システムにおいて提供されている通常番組の視聴以外のサービスを享受することができる。

例えば、オーディオ(楽曲)データのダウンロードサービス用のG U I 画面を表示させて、このG U I 画面を利用して操作を行えば、ユーザが希望した楽曲のオーディオデータをダウンロードしてM D レコーダ/プレーヤ1によりディスクに記録して保存することが可能になる。

ここで、このデジタル衛星放送システムでは、地上局101から衛星102を介してのA Vシステム103への送信を行うに当たり、D S M - C C (デジタル蓄積メディア・コマンド・アンド・コントロール; Digital Storage Media-Command and Control) プロトコルを採用する。

D S M - C C (M P E G - p a r t 6) 方式は、既に知られているように、例えば、何らかのネットワークを介して、デジタル蓄積メディア(D S M)に蓄積されたM P E G 符号化ビットストリームを取り出し(Retrieve)たり、或いはD S M に対してストリームを蓄積(Store)するためのコマンドや制御方式を規定したものである。

そして、D S M - C C 方式によりデータ放送サービス(例えばG

UI画面など)のコンテンツ(オブジェクトの集合)を伝送するためには、コンテンツの記述形式を定義しておく必要がある。このデジタル衛星放送システムでは、コンテンツの記述形式の定義として先に述べたMHEGが採用されている。

このデジタル衛星放送システムにおける地上局101は、図2のように構成されている。

図2に示した地上局101において、テレビ番組素材登録システム131は、テレビ番組素材サーバ106から得られた素材データをAVサーバ135に登録する。この素材データはテレビ番組送出システム139に送られ、ここでビデオデータは例えばMP EG2方式で圧縮され、オーディオデータは、例えばMP EG2オーディオ方式によりパケット化される。テレビ番組送出システム139の出力はマルチプレクサ145に送られる。

また、楽曲素材登録システム132では、楽曲素材サーバ107からの素材データ、つまりオーディオデータを、MP EG2オーディオエンコーダ136A、及びATRACエンコーダ136Bに供給する。MP EG2オーディオエンコーダ136A、ATRACエンコーダ136Bでは、それぞれ供給されたオーディオデータについてエンコード処理(圧縮符号化)を行った後、MP EGオーディオサーバ140A及びATRACオーディオサーバ140Bに登録させる。

MP EGオーディオサーバ140Aに登録されたMP EGオーディオデータは、MP EGオーディオ送出システム143Aに伝送されてここでパケット化された後、マルチプレクサ145に伝送される。ATRACオーディオサーバ140Bに登録されたATRAC

データは、A T R A Cオーディオ送出システム 1 4 3 Bに 4 倍速 A T R A Cデータとして送られ、ここでパケット化されてマルチプレクサ 1 4 5に送出される。

また、音声付加情報登録システム 1 3 3では、音声付加情報サーバ 1 0 8からの素材データである音声付加情報を音声付加情報データベース 1 3 7に登録する。この音声付加情報データベース 1 3 7に登録された音声付加情報は、音声付加情報送出システム 1 4 1に伝送され、同様にして、ここでパケット化されてマルチプレクサ 1 4 5に伝送される。

また、G U I用素材登録システム 1 3 4では、G U Iデータサーバ 1 0 9からの素材データであるG U Iデータを、G U I素材データベース 1 3 8に登録する。

G U I素材データベース 1 3 8に登録されたG U I素材データは、G U Iオーサリングシステム 1 4 2に伝送され、ここで、G U I画面としての出力が可能なデータ形式となるように処理が施される。

つまり、G U Iオーサリングシステム 1 4 2に伝送されてくるデータとしては、例えば、楽曲のダウンロードのためのG U I画面であれば、アルバムジャケットの静止画像データ、歌詞などのテキストデータ、さらには、操作に応じて出力されるべき音声データなどである。

上記した各データはいわゆるモノメディアといわれるが、G U Iオーサリングシステム 1 4 2では、M H E Gオーサリングツールを用いて、これらのモノメディアデータを符号化して、これをオブジェクトとして扱うようにする。

そして、G U I画面の表示態様と操作に応じた画像音声の出力態

様が得られるように上記オブジェクトの関係を規定したシナリオ記述ファイル（スクリプト）と共にM H E G - 5のコンテンツを作成する。

また、テレビ番組素材サーバ106の素材データを基とする画像・音声データ（M P E Gビデオデータ、M P E Gオーディオデータ）と、楽曲素材サーバ107の楽曲素材データを基とするM P E Gオーディオデータ等も、G U I画面に表示され、操作に応じた出力態様が与えられる。

従って、上記シナリオ記述ファイルとしては、上記G U Iオーサリングシステム042では、上記したテレビ番組素材サーバ106の素材データを基とする画像・音声データ、楽曲素材サーバ107の楽曲素材データを基とするM P E Gオーディオデータ、さらには、音声付加情報サーバ108を基とする音声付加情報も必要に応じてオブジェクトとして扱われて、M H E Gのスクリプトによる規定が行われる。

なお、G U Iオーサリングシステム142から伝送されるM H E Gコンテンツのデータとしては、スクリプトファイル、及びオブジェクトとしての各種静止画データファイルやテキストデータファイルなどとなるが、静止画データは、例えばJ P E G (Joint Photograph Experts Group)方式で圧縮された640×480ピクセルのデータとされ、テキストデータは例えば800文字以内のファイルとされる。

G U Iオーサリングシステム142にて得られたM H E GコンテンツのデータはD S M - C Cエンコーダ144に伝送される。

D S M - C Cエンコーダ144では、M P E G 2フォーマットに

従ったビデオ、オーディオデータのデータストリームに多重できる形式のトランスポートストリーム（以下TS(Transport Stream)とも略す）に変換して、パケット化されてマルチプレクサ145に出力される。

マルチプレクサ145においては、テレビ番組送出システム139からのビデオパケット及びオーディオパケットと、MPEGオーディオ送出システム143Aからのオーディオパケットと、ATRA Cオーディオ送出システム143Bからの4倍速オーディオパケットと、音声付加情報送出システム141からの音声付加情報パケットと、GUIオーサリングシステム142からのGUIデータパケットとが時間軸多重化されると共に、キー情報サーバ110から出力されたキー情報に基づいて暗号化される。

マルチプレクサ145の出力は電波送出システム146に伝送され、ここで例えば誤り訂正符号の付加、変調、及び周波数変換などの処理を施された後、アンテナから衛星102に向けて送信される。

図3は、地上局101から衛星102に送信出力される際のデータの一例を示している。なお、この図3に示す各データは実際には時間軸多重化されているものである。また、各データは、図3に示すように、時刻 $t_1$ から時刻 $t_2$ の間が1つのイベントとされ、時刻 $t_2$ から次のイベントとされる。ここでいうイベントとは、例えば音楽番組のチャンネルであれば、複数楽曲のラインナップの組を変更する単位であり、時間的には30分或いは1時間程度となる。

図3に示すように、時刻 $t_1$ から時刻 $t_2$ のイベントでは、通常の動画の番組放送で、所定の内容A1を有する番組が放送されている。また、時刻 $t_2$ から始めるイベントでは、内容A2としての番

組が放送されている。この通常の番組で放送されているのは動画と音声である。

MPEGオーディオチャンネル(1)～(10)は、例えば、チャンネルCH1からCH10の10チャンネル分用意される。このとき、各オーディオチャンネルCH1, CH2, CH3・・・CH10では、1つのイベントが放送されている間は同一楽曲が繰り返し送信される。つまり、時刻 $t_1$ ～ $t_2$ のイベントの期間においては、オーディオチャンネルCH1では楽曲B1が繰り返し送信され、オーディオチャンネルCH2では楽曲C1が繰り返し送信され、以下同様に、オーディオチャンネルCH10では楽曲K1が繰り返し送信されることになる。これは、その下に示されている4倍速ATRAオーディオチャンネル(1)～(10)についても共通である。

つまり、図3において、MPEGオーディオチャンネルと4倍速ATRAオーディオチャンネルのチャンネル番号である( )内の数字が同じものは同じ楽曲となる。また、音声付加情報のチャンネル番号である( )内の数字は、同じチャンネル番号を有するオーディオデータに付加されている音声付加情報である。更に、GUIデータとして伝送される静止画データやテキストデータも各チャンネルごとに形成されるものである。これらのデータは、図4A～図4Dに示すようにMPEG2のトランスポートパケット内で時分割多重されて送信され、図4E～図4Hに示すようにしてIRD112内では各データパケットのヘッダ情報を用いて再構築される。

図5は、本発明に係るデータ伝送システムの構成を示すブロック図である。

このデータ伝送システムは、上述のデジタル衛星放送システムに含まれたAVシステム103を構成するものであって、上記IRD112として機能するデータ送信装置10と上記MDレコーダ/プレーヤ1として機能するデータ受信装置20を備え、上記データ送信装置10とデータ受信装置20が伝送路30を介して接続された構成となっている。

このデータ伝送システムにおいて、上記データ送信装置10は、通信衛星から送られてくる衛星デジタル多チャンネル放送番組を受信するセットトップボックスすなわち上述のIRD112であって、内部バス11に接続された中央演算処理ユニット(CPU: Central Processing Unit)12、メモリ13、入力インターフェース14、ユーザインターフェース15、入出力インターフェース16等により構成されている。上記入力インターフェース14には衛星アンテナ115が接続されている。また、上記入出力インターフェース16は、デジタルインターフェースであるIEEE(The International of Electrical and Electronics Engineers, Inc.)1394ハイ・パフォーマンス・シリアル・バス・インターフェース(以下、単にIEEE1394インターフェースという)であって、IEEE1394バスからなる上記伝送路30に接続されている。

このデータ送信装置10において、上記CPU12は、上記メモリ13に記憶されている制御プログラムにしたがって動作して、上記ユーザインターフェース15を介して入力される操作情報に応じて番組の選局動作等の各種制御動作を行うようになっている。

そして、このデータ送信装置10は、上記受信アンテナ115が接続された上記入力インターフェース14により衛星デジタル多チ



チャンネル放送信号の所望のチャンネルを選局して所望のチャンネルのコンテンツ（音楽データ）及びメタデータ（テキストデータやJPEGデータ等の関連データ）を受信し、受信した音楽データ及びメタデータ（関連データ）を上記入出力インターフェース16から上記伝送路30に送信する。

また、上記データ受信装置20は、上記データ送信装置10すなわちセットトップボックスにより受信したコンテンツ（音楽データ）及びメタデータ（関連データ）を磁気テープや光磁気ディスクなどの記録媒体を介して記録／再生する記録／再生装置であって、内部バス21に接続された中央演算処理ユニット(CPU: Central Processing Unit)22、メモリ23、入出力インターフェース24、ユーザインターフェース25、メディアアクセス部26等により構成されている。上記入出力インターフェース24は、デジタルインターフェースであるIEEE(The International of Electrical and Electronics Engineers, Inc.)1394ハイ・パフォーマンス・シリアル・バス・インターフェース（以下、単にIEEE1394インターフェースという）であって、IEEE1394バスからなる上記伝送路30が接続されている。

図6は、上記伝送路30として実際に用いられるIEEE1394バスケーブルの構造例を示している。

この図6においては、コネクタ600Aと600Bがケーブル601を介して接続されていると共に、ここでは、コネクタ600Aと600Bのピン端子として、ピン番号1～6の6ピンが使用される場合を示している。

コネクタ600A，600Bに設けられる各ピン端子については、

ピン番号 1 は電源 (VP)、ピン番号 2 はグランド (VG)、ピン番号 3 は TPB 1、ピン番号 4 は TPB 2、ピン番号 5 は TPA 1、ピン番号 6 は TPA 2 とされている。

そして、コネクタ 600A-600B 間の各ピンの接続形態は、

ピン番号 1 (VP) - ピン番号 1 (VP)

ピン番号 2 (VG) - ピン番号 2 (VG)

ピン番号 3 (TPB 1) - ピン番号 5 (TPA 1)

ピン番号 4 (TPB 2) - ピン番号 6 (TPA 2)

ピン番号 5 (TPA 1) - ピン番号 3 (TPB 1)

ピン番号 6 (TPA 2) - ピン番号 4 (TPB 2)

のようになっている。そして、上記ピン接続の組のうち、

ピン番号 3 (TPB 1) - ピン番号 5 (TPA 1)

ピン番号 4 (TPB 2) - ピン番号 6 (TPA 2)

の 2 本のツイスト線の組により、差動で信号を相互伝送する信号線 601A を形成し、

ピン番号 5 (TPA 1) - ピン番号 3 (TPB 1)

ピン番号 6 (TPA 2) - ピン番号 4 (TPB 2)

の 2 本のツイスト線の組により、差動で信号を相互伝送する信号線 601B を形成している。

上記 2 組の信号線 601A 及び信号線 601B により伝送される信号は、図 7A に示すデータ信号(Data)と、図 7B に示すストロブ信号(Strobe)である。

図 7A に示すデータ信号は、信号線 601A 又は信号線 601B の一方を使用して TPB 1、TPB 2 から出力され、TPA 1、TPA 2 に入力される。

また、図 7 B に示すストロブ信号は、データ信号と、このデータ信号に同期する伝送クロックとについて所定の論理演算を行うことによって得られる信号であり、実際の伝送クロックよりは低い周波数を有する。このストロブ信号は、信号線 6 0 1 A 又は信号線 6 0 1 B のうち、データ信号伝送に使用していない他方の信号線を使用して、T P A 1, T P A 2 から出力され、T P B 1, T P B 2 に入力される。

例えば、図 7 A, 図 7 B に示すデータ信号及びストロブ信号が、或る I E E E 1 3 9 4 対応の機器に対して入力されたとすると、この機器においては、入力されたデータ信号とストロブ信号とについて所定の論理演算を行って、図 7 C に示すような伝送クロック (C lock) を生成し、所要の入力データ信号処理に利用する。

I E E E 1 3 9 4 規格では、このようなハードウェア的データ伝送形態を採ることで、高速な周期の伝送クロックをケーブルによって機器間で伝送する必要をなくし、信号伝送の信頼性を高めるようにしている。

なお、上記説明では 6 ピンの仕様について説明したが、I E E E 1 3 9 4 フォーマットでは電源 (V P) とグランド (V G) を省略して、2 組のツイスト線である信号線 6 0 1 A 及び信号線 6 0 1 B のみからなる 4 ピンの仕様も存在する。例えば、この A V システム 1 0 3 における M D レコーダ/プレーヤ 1 では、実際には、この 4 ピン仕様のケーブルを用いることで、ユーザにとってより簡易なシステムを提供できるように配慮している。

ここで、I E E E 1 3 9 4 規格では、I E E E 1 3 9 4 バスを介して接続されたネットワーク内で行われる伝送動作をサブアクション

ンと呼び、次の2種類のサブアクションが規定されている。すなわち、2つのサブアクションとして、「アシンクロナス(Asynchronous)データ転送」と呼ばれる通常のデータ伝送を行う非同期伝送モード、及び、「アイソクロナス(Isochronous)データ転送」と呼ばれる伝送帯域を保証した同期伝送モードが定義されている。

すなわち、IEEE 1394規格では、図8に示すようにIsochronous cycle(nominal cycle)の周期を繰り返すことによって送信を行う。この場合、1 Isochronous cycleは、 $125 \mu\text{sec}$ とされ、帯域としては100MHzに相当する。なお、Isochronous cycleの周期としては $125 \mu\text{sec}$ 以外とされても良いことが規定されている。そして、このIsochronous cycle 毎に、データをパケット化して送信する。

このIsochronous cycleの先頭には、1 Isochronous cycleの開始を示すCycle Start Packetが配置される。

このCycle Start Packetは、Cycle Masterとして定義されたIEEE 1394ネットワークシステム内の特定の1機器によってその発生タイミングが指示される。

Cycle Start Packetに続いては、Isochronous Packetが優先的に配置される。Isochronous Packetは、図8のように、チャンネルごとにパケット化された上で時分割的に配列されて転送される(Isochronous subactions)。また、Isochronous subactions内においてパケット毎の区切りには、Isochronous gap といわれる休止区間(例えば $0.05 \mu\text{sec}$ )が設けられる。

このように、IEEE 1394システムでは、1つの伝送線路によってIsochronous データをマルチチャンネルで送受信することが

可能とされている。

ここで、例えばこのAVシステムにおけるMDレコーダ／プレーヤ1が対応するATRA Cデータ（圧縮オーディオデータ）をIsoc hronous 方式により送信することを考えた場合、ATRA Cデータが1倍速の転送レート1.4Mbpsであるとすれば、125μs e cである1Isochronous cycle 周期ごとに、少なくともほぼ20数MバイトのATRA CデータをIsochronous Packetとして伝送すれば、時系列的な連続性（リアルタイム性）が確保されることになる。

例えば、或る機器がATRA Cデータを送信する際には、I E E E 1394ネットワークシステム内のIRM(Isochronous Resource Manager)に対して、ATRA Cデータのリアルタイム送信が確保できるだけの、Isochronous パケットのサイズを要求する。IRMでは、現在のデータ伝送状況を監視して許可／不許可を与え、許可が与えられれば、指定されたチャンネルによって、ATRA CデータをIsochronous Packetにパケット化して送信することができる。これがI E E E 1394インターフェイスにおける帯域予約といわれるものである。

Isochronous cycle の帯域内においてIsochronous subactionsが使用していない残りの帯域を用いて、Asynchronous subactions、即ちAsynchronousのパケット送信が行われる。

図8では、Packet A, Packet B の2つのAsynchronous Packetが送信されている例が示されている。Asynchronous Packet の後には、ack gap(0.05μs e c)の休止期間を挟んで、ACK (Acknowledge) といわれる信号が付随する。ACKは、Asynchronous Trans

actionの過程において、何らかのAsynchronousデータの受信があったことを送信側(Controller)に知らせるためにハードウェア的に受信側(Target)から出力される信号である。

また、Asynchronous Packet 及びこれに続くACKからなるデータ伝送単位の前後には、 $10\mu\text{sec}$ 程度のsubaction gapといわれる休止期間が設けられる。

ここで、Isochronous PacketによりATRA Cデータを送信し、上記ATRA Cデータに付随するAUXデータファイルをAsynchronous Packet により送信するようにすれば、見かけ上、ATRA CデータとAUXデータファイルとを同時に送信することが可能となる。

ここで、Asynchronous伝送は1対1のユニキャスト伝送であり、ブロードキャスト伝送を行うIsochronous 伝送に比べて盗聴が難しいという性質がある。

このデータ伝送システムでは、伝送帯域を確保できるIsochronous 伝送を用いて音楽データを伝送し、関連情報は、Asynchronous伝送を用いて伝送する。

そして、データ受信装置20は、入出力インターフェース24を介して音楽データと関連情報を受信し、それが記録可能であれば、メディアアクセス部26により上記磁気テープや光磁気ディスクなどの記録媒体に記録する。

上記記録媒体に記録された音楽データと関連情報はメディアアクセス部26により再生され、音楽データは、アナログ信号に変換されアナログ音声出力端子26Aから出力され、関連データは映像出力端子26Bから出力される。また、上記メディアアクセス部26

により再生され音楽データと関連情報は、I E E E 1 3 9 4 インターフェイスを介してさらに他の機器に伝送されることがある。

また、データ受信装置 2 0 は、記録禁止の音楽データを受信した場合には、上記メディアアクセス部 2 6 により記録媒体に記録することなく、単に音楽データをアナログ信号に変換してアナログ音声出力端子 2 6 A から出力する。

このデータ受信装置 2 0 において、上記 C P U 2 2 は、上記メモリ 2 3 に記憶されている制御プログラムにしたがって動作して、上記ユーザインターフェイス 2 5 を介して入力される操作情報に応じて、上記メディアアクセス部 2 6 による記録動作等の各種制御動作を行うようになっている。

そして、このデータ伝送システムでは、受信アンテナ 1 1 5 を介してデータ送信装置 1 0 により受信した所望のチャンネルのコンテンツ（音楽データ）及びメタデータ（関連データすなわちテキストデータや J P E G データ等）を、それぞれ別の暗号方式、暗号鍵を用いて暗号化してデータ受信装置 2 0 に伝送する。

すなわち、データ送信装置 1 0 の要部構成を図 9 に示してあるように、上記データ送信装置 1 0 の入力インターフェイス 1 4 は、衛星デジタル多チャンネル放送信号の所望のチャンネルを選局するデマルチプレクサ (DEMUX) 1 4 A と、このデマルチプレクサ (DEMUX) 1 4 A により選局された所望のチャンネルのトランスポートストリームを復号するデコーダ (DEC) 1 4 B を備え、また、入出力インターフェイス 1 6 は、上記デコーダ (DEC) 1 4 B により復号された所望のチャンネルのトランスポートストリームに含まれているコンテンツ（音楽データ）及びメタデータ（関連データすなわちテキストデ

ータやJ P E Gデータ等)を分離するデータ分離回路16Aと、このデータ分離回路16Aにより分離されたコンテンツ(音楽データ)を暗号鍵Kisoにより第1の暗号方式で暗号化してIsochronous Packetを生成する第1のエンコーダ16Bと、上記データ分離回路16Aにより分離されたメタデータ(関連データ)を暗号鍵Kasyncにより第2の暗号方式で暗号化してAsynchronous Packetを生成する第1のエンコーダ16Cを備える。

そして、上記データ送信装置10における入出力インターフェース16は、CPU12により制御されて、図10のフローチャートに示すように動作する。すなわち、上記入出力インターフェース16は、上記入力インターフェース14を介して受信された所望のチャンネルのトランスポートストリームが入力されると(ステップS1)、入力されたトランスポートストリームに含まれているデータがコンテンツ(音楽データ)であるかメタデータ(関連データ)であるかを判定し(ステップS2)、コンテンツ(音楽データ)である場合には、そのコンテンツ(音楽データ)を暗号鍵Kisoにより第1の暗号方式で暗号化し(ステップS3)、第1の暗号方式で暗号化したコンテンツ(音楽データ)をIsochronous Packetとして伝送する処理を行う(ステップS4)。また、入力されたトランスポートストリームに含まれているデータがメタデータ(関連データ)である場合には、そのメタデータ(関連データ)を暗号鍵Kasyncにより第2の暗号方式で暗号化し(ステップS5)、第2の暗号方式で暗号化したメタデータ(関連データ)をAsynchronous Packetとして伝送する処理を行う(ステップS6)。

このデータ伝送システムでは、上記データ伝送に先立って、デー



タ送信装置 10 とデータ受信装置 20 の間で相互認証と、Isochronous 用と Asynchronous 用の 2 種類の暗号鍵の共有プロトコルを実行する。具体的には、図 11 のフローチャートに示すような認証・鍵共有プロトコルを実行してから、データ伝送を行う。なお、このデータ伝送システムにおけるデータ送信装置 10 側の処理手順を図 12 のフローチャートに示すとともに、データ受信装置 20 側の処理手順を図 13 のフローチャートに示す。

上記認証・鍵共有プロトコルを示す図 11 では、データ送信装置 10 を Source Device A で表し、データ受信装置 20 を Sink Device B で表す。これらの機器は、自分が正当であることを示す情報  $K_v$  が機器の製造時に与えられ、秘密に保持している。

そして、このデータ伝送システムにおいて、上記データ送信装置 10 すなわちセットトップボックスの CPU 12 は、先ず、データの伝送を開始するためのスタートコマンドを上記入出力インターフェース 16 から上記伝送路 30 を介してデータ受信装置 20 に送信する（ステップ S10）。

上記データ受信装置 20 すなわち記録装置の CPU 22 は、上記入出力インターフェース 24 に接続された上記伝送路 30 を介して上記データ送信装置 10 から送られてくるスタートコマンド (START command) を受信したら（ステップ S20）、認証・鍵共有プロトコルの開始要求 (Request authentication) と  $m$ （例えば  $m = 64$ ）ビットの 2 つの乱数  $B_{n1}$ ,  $B_{n2}$  を生成して上記データ送信装置 10 に入出力インターフェース 24 を介して送る（ステップ S21）。

上記データ送信装置 10 の CPU 12 は、上記入出力インターフ

エース 16 に接続された上記伝送路 30 を介して上記データ受信装置 20 から送られてくる認証・鍵共有プロトコルの開始要求(Request authentication)と乱数  $B_{n1}$ ,  $B_{n2}$  を受信したら (ステップ S11)、 $m$  ビットの 2 つの乱数  $A_{n1}$ ,  $A_{n2}$  を生成して上記データ受信装置 10 に入出力インターフェース 16 を介して送る (ステップ S12)。

上記データ受信装置 20 は、上記データ送信装置 10 から送られてくる 2 つの乱数  $A_{n1}$ ,  $A_{n2}$  を受信する (ステップ S22)。

そして、上記データ送信装置 10 の CPU12 は、自分が正当であることを示す情報  $K_v$  と上記ステップ S12 でデータ受信装置 20 に送った乱数  $A_{n2}$  と上記ステップ S11 で受信した乱数  $B_{n2}$  を連結した連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) をハッシュ関数 Hash [] に入力し、

$$R2 = \text{Hash} [K_v \parallel A_{n2} \parallel B_{n2}]_{\text{msb}_m}$$

その出力の最上位  $m$  ビットをレスポンスデータ  $R2$  とし、このレスポンスデータ  $R2$  を上記データ受信装置 20 に入出力インターフェース 16 を介して送る (ステップ S13)。図 11 及び図 12 の例では、 $m = 64$  ビットの例を示している。ここで、 $X \parallel Y$  は、 $X$  と  $Y$  とのビット連結を示す。なお、上記レスポンスデータ  $R2$  を与える上記最上位  $m$  ビットは、上記乱数のビット数  $m$  と同じビット数にしているが、上記乱数のビット数  $m$  と違っていてもよい。

上記データ受信装置 20 の CPU22 は、上記データ送信装置 10 から送られてくるレスポンスデータ  $R2$  を受信し (ステップ S23)、自分が正当であることを示す情報  $K_v$  と上記ステップ S22

で受信した乱数  $A_{n1}$  と上記ステップ S 2 1 でデータ送信装置 1 0 に送った乱数  $B_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) をハッシュ関数  $Hash[]$  に入力し、

$$R_1 = Hash[K_v \parallel A_{n1} \parallel B_{n1}]_{msb_m}$$

その出力の最上位  $m$  ビットをレスポンスデータ  $R_1$  とし、このレスポンスデータ  $R_1$  を上記データ送信装置 1 0 に入出力インターフェース 2 4 を介して送る (ステップ S 2 4)。図 1 1 及び図 1 3 の例では、 $m = 64$  ビットの例を示している。なお、上記レスポンスデータ  $R_1$  を与える上記最上位  $m$  ビットも、上記乱数のビット数  $m$  と同じビット数にしてあるが、上記乱数のビット数  $m$  と違っていてもよい。

上記データ送信装置 1 0 の CPU 1 2 は、上記データ受信装置 2 0 から送られてくるレスポンスデータ  $R_1$  を受信する (ステップ S 1 4)。

さらに、上記データ送信装置 1 0 の CPU 1 2 は、自分が正当であることを示す情報  $K_v$  と上記ステップ S 1 2 でデータ受信装置 2 0 に送った乱数  $A_{n1}$  と上記ステップ S 1 1 で受信した乱数  $B_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) を生成し、この連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) をハッシュ関数  $Hash[]$  に入力し、

$$R'_1 = Hash[K_v \parallel A_{n1} \parallel B_{n1}]_{msb_m}$$

その出力の最上位  $m$  ビットを参照データ  $R'_1$  とする (ステップ S 1 5)。すなわち、上記レスポンスデータ  $R_1$  と同じ  $m$  ビットが参照データ  $R'_1$  とされる。

そして、上記データ送信装置 10 の CPU 12 は、上記参照データ  $R'1$  を上記ステップ S 14 で受信したレスポンスデータ  $R1$  と比較する（ステップ S 16）。このステップ S 16 において、レスポンスデータ  $R1$  が参照データ  $R'1$  と一致しなければ、上記データ送信装置 10 の CPU 12 は、上記データ受信装置 20 が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

上記ステップ S 16 においてレスポンスデータ  $R1$  が参照データ  $R'1$  と一致した場合には、上記データ送信装置 10 の CPU 12 は、上記データ受信装置 20 を正当な機器であると判断し、自分が正当であることを示す情報  $Kv$  と上記ステップ S 12 でデータ受信装置 20 に送った乱数  $An1$  と上記ステップ S 11 で受信した乱数  $Bn1$  を連結した連結データ ( $Kv \parallel An1 \parallel Bn1$ ) をハッシュ関数  $Hash[]$  に入力し、

$$Kiso = Hash[Kv \parallel An1 \parallel Bn1]_{lsb\_m}$$

その出力の最下位  $m$  ビットを Isochronous 伝送で送るデータを暗号化するために使用する暗号鍵  $Kiso$  とする。また、上記データ送信装置 10 の CPU 12 は、自分が正当であることを示す情報  $Kv$  と上記ステップ S 12 でデータ受信装置 20 に送った乱数  $An2$  と上記ステップ S 11 で受信した乱数  $Bn2$  を連結した連結データ ( $Kv \parallel An2 \parallel Bn2$ ) をハッシュ関数  $Hash[]$  に入力し、

$$Kasync = Hash[Kv \parallel An2 \parallel Bn2]_{lsb\_m}$$

その出力の最下位  $m$  ビットを Asynchronous 伝送で送るデータを暗号化するために使用する暗号鍵  $Kasync$  とする（ステップ S 17）。

なお、上記 2 種類の暗号鍵  $Kiso$  ,  $Kasync$  を与える上記最下位  $m$  ビットも、上記乱数のビット数  $m$  と同じビット数にしてあるが、

上記乱数のビット数 $m$ と違っていてもよい。

一方、上記データ受信装置 20 の CPU 22 は、自分が正当であることを示す情報  $K_v$  と上記ステップ S 22 で受信した乱数  $A_{n2}$  と上記ステップ S 21 でデータ送信装置 10 に送った乱数  $B_{n2}$  を連結した連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) をハッシュ関数  $Hash[]$  に入力し、

$$R'_2 = Hash[K_v \parallel A_{n2} \parallel B_{n2}]_{msb\_m}$$

その出力の最上位 $m$ ビットを参照データ  $R'_2$  とする (ステップ S 25)。すなわち、上記レスポンスデータ  $R_2$  と同じ $m$ ビットが参照データ  $R'_2$  とされる。

そして、上記データ受信装置 20 の CPU 22 は、この参照データ  $R'_2$  を上記ステップ S 23 で受信したレスポンスデータ  $R_2$  と比較する (ステップ S 26)。このステップ S 26 において、レスポンスデータ  $R_2$  が参照データ  $R'_2$  と一致しなければ、上記データ受信装置 20 の CPU 22 は、上記データ送信装置 10 が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

また、上記ステップ S 26 においてレスポンスデータ  $R_2$  が参照データ  $R'_2$  と一致した場合には、上記データ受信装置 20 の CPU 22 は、上記データ送信装置 10 を正当な機器であると判断し、自分が正当であることを示す情報  $K_v$  と上記ステップ S 22 で受信した乱数  $A_{n1}$  と上記ステップ S 21 でデータ送信装置 10 に送った乱数  $B_{n1}$  を連結した連結データ ( $K_v \parallel A_{n1} \parallel B_{n1}$ ) をハッシュ関数  $Hash[]$  に入力し、

$$K'_{iso} = Hash[K_v \parallel A_{n1} \parallel B_{n1}]_{lsb\_m}$$

その出力の最下位 $m$ ビットを Isochronous 伝送で送られてくるデー

タを復号するために使用する暗号鍵 $K'_{iso}$ とする。すなわち、上記暗号鍵 $K_{iso}$ と同じ $m$ ビットが暗号鍵 $K'_{iso}$ とされる。

また、自分が正当であることを示す情報 $K_v$ と上記ステップ $S_{22}$ で受信した乱数 $A_{n2}$ と上記ステップ $S_{21}$ でデータ送信装置 $10$ に送った乱数 $B_{n2}$ を連結した連結データ( $K_v \parallel A_{n2} \parallel B_{n2}$ )をハッシュ関数 $Hash[]$ に入力し、

$$K'_{async} = Hash[K_v \parallel A_{n2} \parallel B_{n2}]_{lsb_m}$$

その出力の最下位 $m$ ビットをAsynchronous伝送で送られてくるデータを復号するために使用する暗号鍵 $K'_{async}$ とする（ステップ $S_{27}$ ）。すなわち、上記暗号鍵 $K_{async}$ と同じ $m$ ビットが暗号鍵 $K'_{async}$ とされる。

このデータ伝送システムでは、データ伝送に先立って、上記認証・鍵共有プロトコルをデータ送信装置 $10$ とデータ受信装置 $20$ の間でIEEE 1394のAsynchronous伝送によって実行することにより、データ送信装置 $10$ とデータ受信装置 $20$ が、相互に正当性を認証するとともに、Isochronous伝送で暗号化したデータを送るための暗号鍵とAsynchronous伝送で暗号化したデータを送るための暗号鍵を共有することができる。

そして、このデータ伝送システムでは、上記認証・鍵共有プロトコルを実行した後に、データ送信装置 $10$ から音楽データを暗号鍵 $K_{iso}$ で暗号化してIsochronous伝送で送信し、また、関連データを暗号鍵 $K_{async}$ で暗号化してAsynchronous伝送で送信し（ステップ $S_{18}$ ）、データ受信装置 $20$ は、Isochronous伝送により送られてくる音楽データを暗号鍵 $K'_{iso}$ で復号し、また、Asynchronous伝送で送られてくる関連データを暗号鍵 $K'_{async}$ で復号する（ステ

ップS 2 8)。

すなわち、上記認証・鍵共有プロトコルの実行後は、データ受信装置20は、データ送信装置10からIsochronous 伝送により送られてくる音楽データを暗号鍵K'isoで復号し、また、Asynchronous 伝送で送られてくる関連データを暗号鍵K'asyncで復号して、それぞれの平文データを得ることができる。

〔認証・鍵共有プロトコルの他の実施の形態〕

次に、このデータ伝送システムにおいて、上記データ伝送に先立って実行する認証・鍵共有プロトコルの他の例を図14のフローチャートに示す。この場合のデータ送信装置10側の処理手順を図15のフローチャートに示すとともに、データ受信装置20側の処理手順を図16のフローチャートに示す。

上記認証・鍵共有プロトコルを示す図14では、データ送信装置10をSource DeviceAで表し、データ受信装置20をSink DeviceB で表す。これらの機器は、自分が正当であることを示す情報Kvが機器の製造時に与えられ、秘密に保持している。

そして、このデータ伝送システムにおいて、上記データ送信装置10すなわちセットトップボックスのCPU12は、先ず、データの伝送を開始するためのスタートコマンドを上記入出力インターフェース16から上記伝送路30を介してデータ受信装置20に送信する(ステップS110)。

上記データ受信装置20すなわち記録装置のCPU22は、上記入出力インターフェース24に接続された上記伝送路30を介して上記データ送信装置10から送られてくるスタートコマンド(START command)を受信したら(ステップS120)、認証・鍵共有プロ

トコルの開始要求(Request authentication)と $m$  (例えば $m = 64$ ) ビットの2つの乱数 $B_{n1}$ ,  $B_{n2}$ を生成して上記データ送信装置10に入出力インターフェース24を介して送る(ステップS121)。

上記データ送信装置10のCPU12は、上記入出力インターフェース16に接続された上記伝送路30を介して上記データ受信装置20から送られてくる認証・鍵共有プロトコルの開始要求(Request authentication)と乱数 $B_{n1}$ ,  $B_{n2}$ を受信したら(ステップS111)、 $m$ ビットの2つの乱数 $A_{n1}$ ,  $A_{n2}$ を生成して上記データ受信装置20に入出力インターフェース16を介して送る(ステップS112)。

上記データ受信装置20は、上記データ送信装置10から送られてくる2つの乱数 $A_{n1}$ ,  $A_{n2}$ を受信する(ステップS122)。

そして、上記データ送信装置10のCPU12は、自分が正当であることを示す情報 $K_v$ と上記ステップS112でデータ受信装置20に送った乱数 $A_{n1}$ と上記ステップS111で受信した乱数 $B_{n1}$ を連結した連結データ( $K_v \parallel A_{n1} \parallel B_{n1}$ )を生成し、この連結データ( $K_v \parallel A_{n1} \parallel B_{n1}$ )をハッシュ関数Hash[]に

$$R'1 = \text{Hash}[K_v \parallel A_{n1} \parallel B_{n1}]_{\text{msb}_p}$$

その出力の最上位 $p$ ビット(例えば $p = 64$ )を参照データ $R'1$ とするとともに、

$$K_{\text{iso}} = \text{Hash}[K_v \parallel A_{n1} \parallel B_{n1}]_{\text{lsb}_n}$$

最下位 $n$ (例えば $n = 64$ )ビットをIsochronous 伝送で送るデータを暗号化するために使用する暗号鍵 $K_{\text{iso}}$ とする(ステップS1



13)。ここで、 $X \parallel Y$ は、 $X$ と $Y$ とのビット連結を示す。

そして、上記データ送信装置10のCPU12は、このようにして算出した暗号鍵 $K_{iso}$ と上記ステップS112でデータ受信装置20に送った乱数 $A_{n2}$ と上記ステップS111で受信した乱数 $B_{n2}$ を連結した連結データ( $K_{iso} \parallel A_{n2} \parallel B_{n2}$ )を生成し、この連結データ( $K_{iso} \parallel A_{n2} \parallel B_{n2}$ )をハッシュ関数 $Hash$  [ ] に入力し、

$$R_2 = Hash [K_{iso} \parallel A_{n2} \parallel B_{n2}]_{msb\_p}$$

その出力の最上位 $p$ ビットをレスポンスデータ $R_2$ とする(ステップS114)。

そして、上記データ送信装置10のCPU12は、ステップS114で算出したレスポンスデータ $R_2$ を上記データ受信装置20に入出力インターフェース16を介して送る(ステップS115)。

一方、上記データ受信装置20のCPU22は、自分が正当であることを示す情報 $K_v$ と上記ステップS122で受信した乱数 $A_{n1}$ と上記ステップS121でデータ送信装置10に送った乱数 $B_{n1}$ を連結した連結データ( $K_v \parallel A_{n1} \parallel B_{n1}$ )を生成し、この連結データ( $K_v \parallel A_{n1} \parallel B_{n1}$ )をハッシュ関数 $Hash$  [ ] に入力し、

$$R_1 = Hash [K_v \parallel A_{n1} \parallel B_{n1}]_{msb\_p}$$

その出力の最上位 $p$ ビットをレスポンスデータ $R_1$ とし、

$$K'_{iso} = Hash [K_v \parallel A_{n1} \parallel B_{n1}]_{lsb\_n}$$

最下位 $n$ ビットをIsochronous 伝送で送られてくるデータを復号するために使用する暗号鍵 $K'_{iso}$ とする(ステップS123)。

また、上記データ受信装置20のCPU22は、このようにして

算出した暗号鍵  $K'_{iso}$  と上記ステップ S 1 2 2 で受信した乱数  $A_{n2}$  と上記ステップ S 1 2 1 でデータ送信装置 1 0 に送った乱数  $B_{n2}$  を連結した連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) を生成し、この連結データ ( $K_v \parallel A_{n2} \parallel B_{n2}$ ) をハッシュ関数  $Hash[]$  に入力し、

$$R'_2 = Hash[K'_{iso} \parallel A_{n2} \parallel B_{n2}]_{msb_p}$$

その出力の最上位  $p$  ビットを参照データ  $R'_2$  とする (ステップ S 1 2 4)。

上記データ受信装置 2 0 の CPU 2 2 は、上記データ送信装置 1 0 から送られてくるレスポンスデータ  $R_2$  を受信し (ステップ S 1 2 5)、上記ステップ S 1 2 4 で算出した参照  $R'_2$  と比較する (ステップ S 1 2 6)。このステップ S 1 2 6 において、レスポンスデータ  $R_1$  が参照データ  $R'_1$  と一致しなければ、上記データ受信装置 2 0 の CPU 2 2 は、上記データ送信装置 1 0 が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

上記ステップ S 1 2 6 においてレスポンスデータ  $R_2$  が参照データ  $R'_2$  と一致した場合には、上記データ受信装置 2 0 の CPU 2 2 は、上記ステップ S 1 2 3 で算出したレスポンスデータ  $R_1$  を上記データ送信装置 1 0 に入出力インターフェース 1 6 を介して送る (ステップ S 1 2 7)。

上記データ送信装置 1 0 の CPU 1 0 は、上記データ受信装置 2 0 から送られてくるレスポンスデータ  $R_1$  を受信し (ステップ S 1 1 6)、上記ステップ S 1 1 3 で算出した参照データ  $R'_1$  と比較する (ステップ S 1 1 7)。このステップ S 1 1 7 において、レスポンスデータ  $R_1$  が参照データ  $R'_1$  と一致しなければ、上記デー

タ送信装置 20 の CPU 12 は、上記データ受信装置 20 が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

上記ステップ S 117 においてレスポンスデータ R 1 が参照データ R' 1 と一致した場合には、上記データ送信装置 10 の CPU 12 は、上記データ受信装置 20 を正当な機器であると判断し、上記ステップ S 113 で算出した暗号鍵 K<sub>iso</sub> と上記ステップ S 112 でデータ受信装置 20 に送った乱数 A<sub>n2</sub> と上記ステップ S 111 で受信した乱数 B<sub>n2</sub> を連結した連結データ (K<sub>iso</sub> || A<sub>n2</sub> || B<sub>n2</sub>) を生成し、この連結データ (K<sub>iso</sub> || A<sub>n2</sub> || B<sub>n2</sub>) をハッシュ関数 Hash [] に入力し、

$$K_{\text{async}} = \text{Hash} [K_{\text{iso}} \parallel A_{n2} \parallel B_{n2}] \text{lsb}_q$$

その出力の最下位 q ビット (例えば q = 64) を Asynchronous 伝送で送るデータを暗号化するために使用する暗号鍵 K<sub>async</sub> とする (ステップ S 118)。

また、上記データ受信装置 20 の CPU 22 は、上記ステップ S 123 で算出した暗号鍵 K' <sub>iso</sub> と上記ステップ S 122 で受信した乱数 A<sub>n2</sub> と上記ステップ S 121 でデータ送信装置 10 に送った乱数 B<sub>n2</sub> を連結した連結データ (K' <sub>iso</sub> || A<sub>n2</sub> || B<sub>n2</sub>) を生成し、この連結データ (K' <sub>iso</sub> || A<sub>n2</sub> || B<sub>n2</sub>) をハッシュ関数 Hash [] に入力し、

$$K'_{\text{async}} = \text{Hash} [K'_{\text{iso}} \parallel A_{n2} \parallel B_{n2}] \text{lsb}_q$$

その出力の最下位 q ビットを Asynchronous 伝送で送られてくるデータを復号するために使用する暗号鍵 K' <sub>async</sub> とする (ステップ S 128)。

このデータ伝送システムでは、データ伝送に先立って、上記認証

・鍵共有プロトコルをデータ送信装置 10 とデータ受信装置 20 の間で I E E E 1 3 9 4 の Asynchronous 伝送によって実行することにより、データ送信装置 10 とデータ受信装置 20 が、相互に正当性を認証するとともに、Isochronous 伝送で暗号化したデータを送るための暗号鍵と Asynchronous 伝送で暗号化したデータを送るための暗号鍵を共有することができる。

すなわち、上記認証・鍵共有プロトコルの実行後は、データ送信装置 10 から音楽データを暗号鍵 K<sub>iso</sub> で暗号化して Isochronous 伝送で送信し、また、関連データを暗号鍵 K<sub>async</sub> で暗号化して Asynchronous 伝送で送信することによって（ステップ S 1 1 9）、データ受信装置 20 は、Isochronous 伝送により送られてくる音楽データを暗号鍵 K'<sub>iso</sub> で復号し、また、Asynchronous 伝送で送られてくる関連データを暗号鍵 K'<sub>async</sub> で復号することにより（ステップ S 1 2 9）、それぞれの平文データを得ることができる。

ここで、一般に Isochronous 伝送と Asynchronous 伝送では性質が違うので、それぞれに用いられる暗号アルゴリズムやモードもそれぞれに適したものが使用される。そこで、Asynchronous 伝送に使用される暗号アルゴリズムが Isochronous 伝送に使用されるものに比べて強度的に弱い場合、Asynchronous 伝送に使用される暗号鍵 K<sub>async</sub> は、Isochronous 伝送に使用される暗号鍵 K<sub>iso</sub> に比べて比較的容易に露呈してしまうことになる。図 1 1 に示した認証・鍵共有プロトコルでは、各機器が秘密に保持している自分が正当であることを示す情報 K<sub>v</sub> から暗号鍵 K<sub>async</sub> と暗号鍵 K<sub>iso</sub> を直接生成しているので、暗号鍵 K<sub>async</sub> が露呈してしまうと、例えば総当たり攻撃により情報 K<sub>v</sub> が露呈してしまうことになる。

これに対して、図 1 4 に示した認証・鍵共有プロトコルでは、各機器が秘密に保持している自分が正当であることを示す情報  $K_v$  から暗号鍵  $K_{iso}$  を生成し、この暗号鍵  $K_{iso}$  から暗号鍵  $K_{async}$  を生成しているので、暗号鍵  $K_{async}$  が露呈しても、攻撃者は、一方向性関数  $H a s h$  を一度攻撃するだけでは情報  $K_v$  を得ることはできず、総当たり攻撃により暗号鍵  $K_{iso}$  を求めて、しかる後に情報  $K_v$  を総当たり攻撃しなければならない。

すなわち、図 1 4 に示した認証・鍵共有プロトコルでは、図 1 1 に示した認証・鍵共有プロトコルと比較して、各機器が秘密に保持している自分が正当であることを示す情報  $K_v$  が露呈しにくく、伝送帯域の保証が必要なデータと上記データに関する関連データを安全にかつ確実に伝送することができる。

なお、図 1 4 に示した認証・鍵共有プロトコルでは、上述のデータ伝送システムでは、Isochronous 伝送に使用される暗号鍵  $K_{iso}$  に基づいて、Asynchronous 伝送に使用される暗号鍵  $K_{async}$  を生成するようにしたが、逆に、Asynchronous 伝送に使用される暗号鍵  $K_{async}$  を情報  $K_v$ 、乱数  $A_{n1}$ 、乱数  $B_{n1}$  から生成し、生成された暗号鍵  $K_{async}$ 、乱数  $A_{n2}$ 、乱数  $B_{n2}$  から Isochronous 伝送に使用される暗号鍵  $K_{iso}$  を生成するように構成しても良い。

また、図 1 4 に示した認証・鍵共有プロトコルでは、データ送信装置 1 0 で暗号鍵  $K_{iso}$  から生成したデータをレスポンスデータ  $R_2$  としてデータ受信装置 2 0 に送信し、データ受信装置 2 0 で情報  $K_v$  から生成したデータをレスポンスデータ  $R_1$  としてデータ送信装置 1 0 に送信するように構成したが、データ送信装置 1 0 が情報  $K_v$  から生成したデータをレスポンスデータ  $R_2$  としてデータ受信

装置 20 に送信し、データ受信装置 20 が暗号鍵  $K_{iso}$  から生成したデータをレスポンスデータ  $R_1$  としてデータ送信装置 10 に送信するように構成しても良い。

なお、上述のデータ伝送システムでは、各認証・鍵共有プロトコルを実行することによりデータ送信装置 10 とデータ受信装置 20 の間で共有される暗号鍵  $K_{iso}$ 、 $K'_{iso}$  及び暗号鍵  $K_{async}$ 、 $K'_{async}$  を用いて伝送データを暗号化／復号するようにしているが、実際に伝送するデータを暗号化／復号するための暗号鍵（コンテンツキー）は別に用意して、暗号鍵  $K_{iso}$ 、 $K'_{iso}$  及び暗号鍵  $K_{async}$ 、 $K'_{async}$  を用いてコンテンツキーをデータ送信装置 10 とデータ受信装置 20 の間で共有することもできる。

以上のように本実施の形態では、伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースを介して、伝送帯域の保証が必要なデータを第 1 の伝送モードで伝送し、上記データに関する関連データを第 2 の伝送モードで伝送するので、伝送帯域が確保された伝送方式と伝送帯域が確保されていない伝送方式の 2 種類の伝送方式を採用して、データを確実に伝送することができる。

また、上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で暗号化して第 1 の伝送モードで伝送し、上記データに関する関連データを第 2 の暗号鍵で暗号化して第 2 の伝送モードで伝送するにより、伝送帯域の保証が必要なデータと上記データに関する関連データを安全に伝送することができる。

さらに、データ伝送に先立って、データ送信装置とデータ受信装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコル

を実行することによって、データ送信装置とデータ受信装置が互いの正当性を認証するとともに、暗号鍵を共有することができ、伝送帯域の保証が必要なデータと上記データに関する関連データを安全にかつ確実に伝送することができる。

### 請求の範囲

1. 伝送帯域が保証された第1の伝送モードと伝送帯域が保証されていない第2の伝送モードを持つインターフェースと、上記伝送帯域の保証が必要なデータを第1の暗号鍵で暗号化して第1の伝送モードで上記インターフェースを介して送信し、上記データに関する関連データを第2の暗号鍵で暗号化して第2の伝送モードで上記インターフェースを介して送信する送信制御手段とを備える第1の情報処理装置と、

伝送帯域が保証された第1の伝送モードと伝送帯域が保証されていない第2の伝送モードを持つインターフェースと、上記インターフェースを介して第1の伝送モードで受信される上記伝送帯域の保証が必要なデータを第1の暗号鍵で復号し、上記インターフェースを介して第2の伝送モードで受信される上記関連データを第2の暗号鍵で復号する受信制御手段とを備える第2の情報処理装置と

を具備する情報処理システム。

2. データ伝送に先立って、上記第1の情報処理装置と第2の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する請求の範囲第1項記載の情報処理システム。

3. 音楽データを上記第1の伝送モードで伝送し、上記音楽データに関する関連データを第2の伝送モードで伝送する請求の範囲第1項記載の情報処理システム。

4. 上記第1の情報処理装置と第2の情報処理装置をIEEE(T



he International of Electrical and Electronics Engineers, Inc.) 1394規格に準拠したインターフェースを介して接続し、伝送帯域の保証が必要なデータをアイソクロナス(Isochronous)伝送モードで伝送し、上記データに関する関連データをアシンクロナス(Asynchronous)伝送モードで伝送する請求の範囲第1項記載の情報処理システム。

5. データ伝送に先立って、上記第1の情報処理装置と第2の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス(Asynchronous)伝送モードで実行する請求の範囲第4項記載の情報処理システム。

6. 上記第2の情報処理装置は、2つの乱数を生成して第1の情報処理装置に送信し、

上記第1の情報処理装置は、2つの乱数を生成して上記第2の情報処理装置に送信し、

上記第1の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて第1の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び第2の伝送モードで送信するデータを暗号化するために使用する暗号鍵を生成し、

上記第2の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて第1の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び第2の伝送モードで送られてくるデータを復号するために使用する暗号鍵を生成する請求の範囲第1項の情報処理システム。

7. 上記第1の情報処理装置は、自分が正当な機器であることを

示す情報と上記生成した乱数と受信した乱数とに基づいて生成したデータ P を上記第 2 の情報処理装置に送信し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ Q を上記第 1 の情報処理装置に送信し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ Q' が受信したデータ Q と一致した場合には、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵を生成し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ P' が受信したデータ P と一致した場合には、上記第 1 の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵を生成する請求の範囲第 6 項記載の情報処理システム。

8. 上記第 2 の情報処理装置は、2つの乱数 R 1, R 2 を生成して第 1 の情報処理装置に送信し、

上記第 1 の情報処理装置は、2つの乱数 S 1, S 2 を生成して上記第 2 の情報処理装置に送信し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数 S 2 と受信した乱数 R 2 とに基づいて生成したデータ P を上記第 2 の情報処理装置に送信し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す

情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  とに基づいて生成したデータ  $Q$  を上記第 1 の情報処理装置に送信し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数  $S_1$  と受信した乱数  $R_1$  とに基づいて生成したデータ  $Q'$  が受信したデータ  $Q$  と一致した場合には、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_1$  及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_2$  を生成し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $S_2$  と上記生成した乱数  $R_2$  とに基づいて生成したデータ  $P'$  が受信したデータ  $P$  と一致した場合には、上記第 1 の伝送モードで送信されるデータを復号するために使用する暗号鍵  $K'_1$  及び上記第 2 の伝送モードで送信されるデータを復号するために使用する暗号鍵  $K'_2$  を生成する請求の範囲第 7 項記載の情報処理システム。

9. 上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数  $S_1$  と受信した乱数  $R_1$  を用いて一方向関数を演算した結果を用いて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_1$  を生成すると共に、自分が正当な機器であることを示す情報と上記生成した乱数  $S_2$  と受信した乱数  $R_2$  を用いて一方向関数を演算した結果を用いて、上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_2$  を生成し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  を用いて一方向関

数を演算した結果を用いて、上記第 1 の伝送モードで送信されるデータを復号するために使用する暗号鍵  $K' 1$  を生成すると共に、自分が正当な機器であることを示す情報と受信した乱数  $S 2$  と上記生成した乱数  $R 2$  を用いて一方向関数を演算した結果を用いて、上記第 2 の伝送モードで送信されるデータを復号するために使用する暗号鍵  $K' 2$  を生成する請求の範囲第 8 項記載の情報処理システム。

10. 上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数  $S 2$  と受信した乱数  $R 2$  を用いて一方向関数を演算した結果を用いて生成したデータ  $P$  を上記第 2 の情報処理装置に送信し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $S 1$  と上記生成した乱数  $R 1$  を用いて一方向関数を演算した結果を用いて生成したデータ  $Q$  を上記第 2 の情報処理装置に送信し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数  $S 1$  と受信した乱数  $R 1$  を用いて一方向関数を演算した結果を用いて生成したデータ  $Q'$  が受信したデータ  $Q$  と一致した場合には、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K 1$  及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K 2$  を生成し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $S 2$  と上記生成した乱数  $R 2$  を用いて一方向関数を演算した結果を用いて生成したデータ  $P'$  が受信したデータ  $P$  と一致した場合には、上記第 1 の伝送モードで送信されるデータを復号するために使用する暗号鍵  $K' 1$  及び上記第 2 の伝送モードで

送信されるデータを復号するために使用する暗号鍵  $K' 2$  を生成する請求の範囲第 9 項記載の情報処理システム。

1 1. 上記第 1 の情報処理装置及び上記第 2 の情報処理装置は、一方向関数を演算した結果の一部のビット値を用いて暗号鍵  $K 1$ 、暗号鍵  $K 2$ 、暗号鍵  $K' 1$  及び暗号鍵  $K' 2$  を生成する請求の範囲第 9 項記載の情報処理システム。

1 2. 上記第 1 の情報処理装置及び上記第 2 の情報処理装置は、一方向関数を演算した結果の一部のビット値を用いてデータ  $P$ 、データ  $Q'$ 、データ  $Q$  及びデータ  $P'$  を生成する請求の範囲第 1 1 項記載の情報処理システム。

1 3. 上記第 1 の情報処理装置及び上記第 2 の情報処理装置は、一方向関数を演算した結果の最下位  $n$  ビットを用いて、暗号鍵  $K 1$ 、暗号鍵  $K 2$ 、暗号鍵  $K' 1$  及び暗号鍵  $K' 2$  を生成する請求の範囲第 1 1 項記載の情報処理システム。

1 4. 上記第 1 の情報処理装置及び上記第 2 の情報処理装置は、一方向関数を演算した結果の最上位  $m$  ビットを用いてデータ  $P$ 、データ  $Q'$ 、データ  $Q$  及びデータ  $P'$  を生成する請求の範囲第 1 3 項記載の情報処理システム。

1 5. 上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数  $S 1$  と受信した乱数  $R 1$  を連結した連結データに対して一方向関数を演算した結果を用いて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K 1$  を生成すると共に、自分が正当な機器であることを示す情報と上記生成した乱数  $S 2$  と受信した乱数  $R 2$  を連結した連結データに対して一方向関数を演算した結果を用いて、上記第 2 の伝送モード

で送信するデータを暗号化するために使用する暗号鍵  $K_2$  を生成し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  を連結した連結データに対して一方向関数を演算した結果を用いて、上記第 1 の伝送モードで送信されるデータを復号するために使用する暗号鍵  $K'_1$  を生成すると共に、自分が正当な機器であることを示す情報と受信した乱数  $S_2$  と上記生成した乱数  $R_2$  を連結した連結データに対して一方向関数を演算した結果を用いて、上記第 2 の伝送モードで送信されるデータを復号するために使用する暗号鍵  $K'_2$  を生成する請求の範囲第 8 項記載の情報処理システム。

16. 上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数  $S_2$  と受信した乱数  $R_2$  を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ  $P$  を上記第 2 の情報処理装置に送信し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ  $Q$  を上記第 1 の情報処理装置に送信し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数  $S_1$  と受信した乱数  $R_1$  を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ  $Q'$  が受信したデータ  $Q$  と一致した場合には、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_1$  及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_2$  を生成し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $S_2$  と上記生成した乱数  $R_2$  を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ  $P'$  が受信したデータ  $P$  と一致した場合には、上記第 1 の伝送モードで送信されるデータを復号するために使用する暗号鍵  $K'_1$  及び上記第 2 の伝送モードで送信されるデータを復号するために使用する暗号鍵  $K'_2$  を生成する請求の範囲第 15 項記載の情報処理システム。

17. 上記第 1 の情報処理装置及び上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成し、生成された暗号鍵と上記生成した乱数と受信した乱数とに基づいて、他方の伝送モードの暗号鍵を生成する請求の範囲第 6 項記載の情報処理システム。

18. 上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成すると共に、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータ  $P$  を上記第 2 の情報処理装置に送信し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて、上記第 1 の

伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第2の伝送モードで送られてくるデータを復号するために使用する暗号鍵のいずれか一方の暗号鍵を生成すると共に、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータP'が受信したデータPとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータQを上記第1の情報処理装置に送信すると共に、既に生成されている伝送モード用の暗号鍵と受信した乱数と上記生成した乱数とに基づいて、上記第1の伝送モード及び上記第2の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵を生成し、

上記第1の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータQ'が受信したデータQと一致した場合には、既に生成されている伝送モード用の暗号鍵と受信した乱数と上記生成した乱数とに基づいて、上記第1の伝送モード及び上記第2の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵を生成する請求の範囲第17項記載の情報処理システム。

19. 上記第2の情報処理装置は、2つの乱数R1, R2を生成して第1の情報処理装置に送信し、

上記第1の情報処理装置は、2つの乱数S1, S2を生成して上記第2の情報処理装置に送信し、

上記第1の情報処理装置は、自分が正当な機器であることを示す



情報と受信した乱数  $R_1$  と上記生成した乱数  $S_1$  とに基づいて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵  $K_1$  を生成すると共に、上記生成された暗号鍵  $K_1$  と受信した乱数  $R_2$  と上記生成した乱数  $S_2$  とに基づいて生成したデータ  $P$  を上記第 2 の情報処理装置に送信し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  とに基づいて、上記第 1 の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のいずれか一方の暗号鍵  $K_1'$  を生成すると共に、上記生成された暗号鍵  $K_1'$  と受信した乱数  $S_2$  と上記生成した乱数  $R_2$  とに基づいて生成したデータ  $P'$  と受信したデータ  $P$  とが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  とに基づいて生成したデータ  $Q$  を上記第 1 の情報処理装置に送信すると共に、既に生成されている伝送モード用の暗号鍵  $K_1'$  と受信した乱数  $S_2$  と上記生成した乱数  $S_2$  とに基づいて、上記第 1 の伝送モード及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵  $K_2'$  を生成し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $R_1$  と上記生成した乱数  $S_1$  とに基づいて生成したデータ  $Q'$  が受信したデータ  $Q$  と一致した場合には、既に生成

されている伝送モード用の暗号鍵  $K_1$  と受信した乱数  $R_2$  と上記生成した乱数  $S_2$  とに基づいて、上記第 1 の伝送モード及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵  $K_2$  を生成する請求の範囲第 18 項記載の情報処理システム。

20. 上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $R_1$  と上記生成した乱数  $S_1$  とを用いて一方向関数を演算した結果を用いて暗号鍵  $K_1$  を生成すると共に、生成された暗号鍵  $K_1$  と受信した乱数  $R_2$  と上記生成した乱数  $S_2$  とを用いて一方向関数を演算した結果を用いて暗号鍵  $K_2$  を生成し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  とを用いて一方向関数を演算した結果を用いて暗号鍵  $K_1'$  を生成すると共に、生成された暗号鍵  $K_1'$  と受信した乱数  $S_2$  と上記生成した乱数  $S_2$  とを用いて一方向関数を演算した結果を用いて暗号鍵  $K_2'$  を生成する請求の範囲第 19 項記載の情報処理システム。

21. 上記第 1 の情報処理装置は、上記生成された暗号鍵  $K_1$  と受信した乱数  $R_2$  と上記生成した乱数  $S_2$  とを用いて一方向関数を演算した結果を用いて生成したデータ  $P$  を上記第 2 の情報処理装置に送信し、

上記第 2 の情報処理装置は、上記生成された暗号鍵  $K_1'$  と受信した乱数  $S_2$  と上記生成した乱数  $R_2$  とを用いて一方向関数を演算した結果を用いてデータ  $P'$  と受信したデータ  $P$  とが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  とを用いて一方

向関数を演算した結果を用いて生成したデータ Q を上記第 1 の情報処理装置に送信し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数 R 1 と上記生成した乱数 S 1 とを用いて一方向関数を演算した結果を用いて生成したデータ Q' が受信したデータ Q と一致した場合には、暗号鍵 K 2 を生成する請求の範囲第 20 項記載の情報処理システム。

22. 上記第 1 の情報処理装置及び上記第 2 の情報処理装置は、一方向関数を演算した結果の一部のビット値を用いて暗号鍵 K 1、暗号鍵 K 2、暗号鍵 K' 1 及び暗号鍵 K' 2 を生成する請求の範囲第 20 項記載の情報処理システム。

23. 上記第 1 の情報処理装置及び上記第 2 の情報処理装置は、一方向関数を演算した結果の一部のビット値を用いてデータ P、データ Q'、データ Q 及びデータ P' を生成する請求の範囲第 22 項記載の情報処理システム。

24. 上記第 1 の情報処理装置及び上記第 2 の情報処理装置は、一方向関数を演算した結果の最下位 n ビットを用いて、暗号鍵 K 1、暗号鍵 K 2、暗号鍵 K' 1 及び暗号鍵 K' 2 を生成する請求の範囲第 22 項記載の情報処理システム。

25. 上記第 1 の情報処理装置及び上記第 2 の情報処理装置は、一方向関数を演算した結果の最上位 m ビットを用いてデータ P、データ Q'、データ Q 及びデータ P' を生成する請求の範囲第 24 項記載の情報処理システム。

26. 上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数 R 1 と上記生成した乱数 S 1 を連結した

連結データに対して一方向関数を演算した結果を用いて暗号鍵 K 1 を生成すると共に、生成された暗号鍵 K 1 と受信した乱数 R 2 と上記生成した乱数 S 2 を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵 K 2 を生成し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数 S 1 と上記生成した乱数 R 1 を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵 K 1' を生成すると共に、生成された暗号鍵 K 1' と受信した乱数 S 2 と上記生成した乱数 S 2 を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵 K 2' を生成する請求の範囲第 19 項記載の情報処理システム。

27. 上記第 1 の情報処理装置は、上記生成された暗号鍵 K 1 と受信した乱数 R 2 と上記生成した乱数 S 2 を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ P を上記第 2 の情報処理装置に送信し、

上記第 2 の情報処理装置は、上記生成された暗号鍵 K 1' と受信した乱数 S 2 と上記生成した乱数 R 2 を連結した連結データに対して一方向関数を演算した結果を用いてデータ P' と受信したデータ P とが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数 S 1 と上記生成した乱数 R 1 を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ Q を上記第 1 の情報処理装置に送信し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数 R 1 と上記生成した乱数 S 1 を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ Q

’ が受信したデータ Q と一致した場合には、暗号鍵 K 2 を生成する請求の範囲第 2 6 項記載の情報処理システム。

28. 第 1 の情報処理装置と第 2 の情報処理装置との間で伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースを介してデータ伝送を行う情報処理方法であって、

上記第 1 の情報処理装置から伝送帯域の保証が必要なデータを第 1 の暗号鍵で暗号化して第 1 の伝送モードで送信するとともに、上記データに関する関連データを第 2 の暗号鍵で暗号化して第 2 の伝送モードで送信し、

上記第 2 の情報処理装置側で第 1 の伝送モードで受信される上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で復号し、第 2 の伝送モードで受信される上記関連データを第 2 の暗号鍵で復号する情報処理方法

29. データ伝送に先立って、上記第 1 の情報処理装置と第 2 の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する請求の範囲第 2 8 項記載の情報処理方法。

30. 音楽データを上記第 1 の伝送モードで伝送し、上記音楽データに関する関連データを第 2 の伝送モードで伝送する請求の範囲第 2 8 項記載の情報処理方法。

31. 上記第 1 の情報処理装置と第 2 の情報処理装置との間で、を I E E E (The International of Electrical and Electronics Engineers, Inc.) 1 3 9 4 規格に準拠したインターフェースを介して、伝送帯域の保証が必要なデータをアイソクロナス (Isochronous) 伝送モードで伝送し、上記データに関する関連データをアシンクロナ

ス(Asynchronous)伝送モードで伝送する請求の範囲第28項記載の情報処理方法。

32. データ伝送に先立って、上記第1の情報処理装置と第2の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス(Asynchronous)伝送モードで実行する請求の範囲第31項記載の情報処理方法。

33. 上記第2の情報処理装置は、2つの乱数を生成して第1の情報処理装置に送信し、

上記第1の情報処理装置は、2つの乱数を生成して上記第2の情報処理装置に送信し、

上記第1の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて第1の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び第2の伝送モードで送信するデータを暗号化するために使用する暗号鍵を生成し、

上記第2の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて第1の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び第2の伝送モードで送られてくるデータを復号するために使用する暗号鍵を生成する請求の範囲第28項の情報処理方法。

34. 上記第1の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて生成したデータPを上記第2の情報処理装置に送信し、

上記第2の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデー

タ Q を上記第 1 の情報処理装置に送信し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ Q' が受信したデータ Q と一致した場合には、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵を生成し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ P' が受信したデータ P と一致した場合には、上記第 1 の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵を生成する請求の範囲第 3 3 項記載の情報処理方法。

35. 上記第 2 の情報処理装置は、2つの乱数 R 1, R 2 を生成して第 1 の情報処理装置に送信し、

上記第 1 の情報処理装置は、2つの乱数 S 1, S 2 を生成して上記第 2 の情報処理装置に送信し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数 S 2 と受信した乱数 R 2 とに基づいて生成したデータ P を上記第 2 の情報処理装置に送信し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数 S 1 と上記生成した乱数 R 1 とに基づいて生成したデータ Q を上記第 1 の情報処理装置に送信し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数 S 1 と受信した乱数 R 1 とに基づいて生成

したデータ  $Q'$  が受信したデータ  $Q$  と一致した場合には、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_1$  及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_2$  を生成し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $S_2$  と上記生成した乱数  $R_2$  とに基づいて生成したデータ  $P'$  が受信したデータ  $P$  と一致した場合には、上記第 1 の伝送モードで送信されるデータを復号するために使用する暗号鍵  $K'_1$  及び上記第 2 の伝送モードで送信されるデータを復号するために使用する暗号鍵  $K'_2$  を生成する請求の範囲第 3 4 項記載の情報処理方法。

36. 上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数  $S_1$  と受信した乱数  $R_1$  を用いて一方向関数を演算した結果を用いて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_1$  を生成すると共に、自分が正当な機器であることを示す情報と上記生成した乱数  $S_2$  と受信した乱数  $R_2$  を用いて一方向関数を演算した結果を用いて、上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_2$  を生成し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  を用いて一方向関数を演算した結果を用いて、上記第 1 の伝送モードで送信されるデータを復号するために使用する暗号鍵  $K'_1$  を生成すると共に、自分が正当な機器であることを示す情報と受信した乱数  $S_2$  と上記生成した乱数  $R_2$  を用いて一方向関数を演算した結果を用いて、上記



第2の伝送モードで送信されるデータを復号するために使用する暗号鍵 $K'2$ を生成する請求の範囲第35項記載の情報処理方法。

37. 上記第1の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数 $S2$ と受信した乱数 $R2$ を用いて一方向関数を演算した結果を用いて生成したデータ $P$ を上記第2の情報処理装置に送信し、

上記第2の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数 $S1$ と上記生成した乱数 $R1$ を用いて一方向関数を演算した結果を用いて生成したデータ $Q$ を上記第1の情報処理装置に送信し、

上記第1の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数 $S1$ と受信した乱数 $R1$ を用いて一方向関数を演算した結果を用いて生成したデータ $Q'$ が受信したデータ $Q$ と一致した場合には、上記第1の伝送モードで送信するデータを暗号化するために使用する暗号鍵 $K1$ 及び上記第2の伝送モードで送信するデータを暗号化するために使用する暗号鍵 $K2$ を生成し、

上記第2の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数 $S2$ と上記生成した乱数 $R2$ を用いて一方向関数を演算した結果を用いて生成したデータ $P'$ が受信したデータ $P$ と一致した場合には、上記第1の伝送モードで送信されるデータを復号するために使用する暗号鍵 $K'1$ 及び上記第2の伝送モードで送信されるデータを復号するために使用する暗号鍵 $K'2$ を生成する請求の範囲第36項記載の情報処理方法。

38. 上記第1の情報処理装置及び上記第2の情報処理装置において一方向関数を演算した結果の一部のビット値を用いて暗号鍵 $K$

1、暗号鍵K 2、暗号鍵K' 1 及び暗号鍵K' 2 を生成する請求の範囲第3 6項記載の情報処理方法。

3 9. 上記第1の情報処理装置及び上記第2の情報処理装置において、一方向関数を演算した結果の一部のビット値を用いてデータP、データQ'、データQ 及びデータP' を生成する請求の範囲第3 8項記載の情報処理方法。

4 0. 上記第1の情報処理装置及び上記第2の情報処理装置において、一方向関数を演算した結果の最下位nビットを用いて、暗号鍵K 1、暗号鍵K 2、暗号鍵K' 1 及び暗号鍵K' 2 を生成する請求の範囲第3 8項記載の情報処理方法。

4 1. 上記第1の情報処理装置及び上記第2の情報処理装置において、一方向関数を演算した結果の最上位mビットを用いてデータP、データQ'、データQ 及びデータP' を生成する請求の範囲第4 0項記載の情報処理方法。

4 2. 上記第1の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数S 1と受信した乱数R 1を連結した連結データに対して一方向関数を演算した結果を用いて、上記第1の伝送モードで送信するデータを暗号化するために使用する暗号鍵K 1を生成すると共に、自分が正当な機器であることを示す情報と上記生成した乱数S 2と受信した乱数R 2を連結した連結データに対して一方向関数を演算した結果を用いて、上記第2の伝送モードで送信するデータを暗号化するために使用する暗号鍵K 2を生成し、

上記第2の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数S 1と上記生成した乱数R 1を連結した連結データに対して一方向関数を演算した結果を用いて、上記第1の伝送

モードで送信されるデータを復号するために使用する暗号鍵 $K'1$ を生成すると共に、自分が正当な機器であることを示す情報と受信した乱数 $S2$ と上記生成した乱数 $R2$ を連結した連結データに対して一方向関数を演算した結果を用いて、上記第2の伝送モードで送信されるデータを復号するために使用する暗号鍵 $K'2$ を生成する請求の範囲第35項記載の情報処理方法。

43. 上記第1の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数 $S2$ と受信した乱数 $R2$ を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ $P$ を上記第2の情報処理装置に送信し、

上記第2の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数 $S1$ と上記生成した乱数 $R1$ を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ $Q$ を上記第1の情報処理装置に送信し、

上記第1の情報処理装置は、自分が正当な機器であることを示す情報と上記生成した乱数 $S1$ と受信した乱数 $R1$ を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ $Q'$ が受信したデータ $Q$ と一致した場合には、上記第1の伝送モードで送信するデータを暗号化するために使用する暗号鍵 $K1$ 及び上記第2の伝送モードで送信するデータを暗号化するために使用する暗号鍵 $K2$ を生成し、

上記第2の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数 $S2$ と上記生成した乱数 $R2$ を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ $P'$ が受信したデータ $P$ と一致した場合には、上記第1の伝送モード

で送信されるデータを復号するために使用する暗号鍵 $K'$  1 及び上記第 2 の伝送モードで送信されるデータを復号するために使用する暗号鍵 $K'$  2 を生成する請求の範囲第 4 2 項記載の情報処理方法。

4 4. 上記第 1 の情報処理装置及び上記第 2 の情報処理装置において、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成し、生成された暗号鍵と上記生成した乱数と受信した乱数とに基づいて、他方の伝送モードの暗号鍵を生成する請求の範囲第 3 3 項記載の情報処理方法。

4 5. 上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成すると共に、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータ P を上記第 2 の情報処理装置に送信し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて、上記第 1 の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のいずれか一方の暗号鍵を生成すると共に、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータ P' が受信したデータ P とが一致するか否かを検証し、

一致した場合には、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ Q を上記第 1 の情報処理装置に送信すると共に、既に生成されている伝送モード用の暗号鍵と受信した乱数と上記生成した乱数とに基づいて、上記第 1 の伝送モード及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵を生成し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ Q' が受信したデータ Q と一致した場合には、既に生成されている伝送モード用の暗号鍵と受信した乱数と上記生成した乱数とに基づいて、上記第 1 の伝送モード及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵を生成する請求の範囲第 4 4 項記載の情報処理方法。

46. 上記第 2 の情報処理装置は、2つの乱数 R 1, R 2 を生成して第 1 の情報処理装置に送信し、

上記第 1 の情報処理装置は、2つの乱数 S 1, S 2 を生成して上記第 2 の情報処理装置に送信し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数 R 1 と上記生成した乱数 S 1 とに基づいて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵 K 1 を生成すると共に、上記生成された暗号鍵 K 1 と受信した乱数 R 2 と上記生成した乱数

S 2 とに基づいて生成したデータ P を上記第 2 の情報処理装置に送信し、

上記第 2 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数 S 1 と上記生成した乱数 R 1 とに基づいて、上記第 1 の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のいずれか一方の暗号鍵 K 1' を生成すると共に、上記生成された暗号鍵 K 1' と受信した乱数 S 2 と上記生成した乱数 R 2 とに基づいて生成したデータ P' と受信したデータ P とが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数 S 1 と上記生成した乱数 R 1 とに基づいて生成したデータ Q を上記第 1 の情報処理装置に送信すると共に、既に生成されている伝送モード用の暗号鍵 K 1' と受信した乱数 S 2 と上記生成した乱数 S 2 とに基づいて、上記第 1 の伝送モード及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵 K 2' を生成し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数 R 1 と上記生成した乱数 S 1 とに基づいて生成したデータ Q' が受信したデータ Q と一致した場合には、既に生成されている伝送モード用の暗号鍵 K 1 と受信した乱数 R 2 と上記生成した乱数 S 2 とに基づいて、上記第 1 の伝送モード及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵 K 2 を生成する請求の範囲第 4 5 項記載の情報処理方法。

47. 上記第1の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数R1と上記生成した乱数S1とを用いて一方向関数を演算した結果を用いて暗号鍵K1を生成すると共に、生成された暗号鍵K1と受信した乱数R2と上記生成した乱数S2とを用いて一方向関数を演算した結果を用いて暗号鍵K2を生成し、

上記第2の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数S1と上記生成した乱数R1とを用いて一方向関数を演算した結果を用いて暗号鍵K1'を生成すると共に、生成された暗号鍵K1'と受信した乱数S2と上記生成した乱数S2とを用いて一方向関数を演算した結果を用いて暗号鍵K2'を生成する請求の範囲第46項記載の情報処理方法。

48. 上記第1の情報処理装置は、上記生成された暗号鍵K1と受信した乱数R2と上記生成した乱数S2とを用いて一方向関数を演算した結果を用いて生成したデータPを上記第2の情報処理装置に送信し、

上記第2の情報処理装置は、上記生成された暗号鍵K1'と受信した乱数S2と上記生成した乱数R2とを用いて一方向関数を演算した結果を用いてデータP'と受信したデータPとが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数S1と上記生成した乱数R1とを用いて一方向関数を演算した結果を用いて生成したデータQを上記第1の情報処理装置に送信し、

上記第1の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数R1と上記生成した乱数S1とを用いて一方向関数を演算した結果を用いて生成したデータQ'が受信したデータ

Qと一致した場合には、暗号鍵K 2を生成する請求の範囲第4 7項記載の情報処理方法。

4 9. 上記第1の情報処理装置及び上記第2の情報処理装置において、一方向関数を演算した結果の一部のビット値を用いて暗号鍵K 1、暗号鍵K 2、暗号鍵K' 1及び暗号鍵K' 2を生成する請求の範囲第4 7項記載の情報処理方法。

5 0. 上記第1の情報処理装置及び上記第2の情報処理装置において、一方向関数を演算した結果の一部のビット値を用いてデータP、データQ'、データQ及びデータP'を生成する請求の範囲第4 9項記載の情報処理方法。

5 1. 上記第1の情報処理装置及び上記第2の情報処理装置において、一方向関数を演算した結果の最下位nビットを用いて、暗号鍵K 1、暗号鍵K 2、暗号鍵K' 1及び暗号鍵K' 2を生成する請求の範囲第4 9項記載の情報処理方法。

5 2. 上記第1の情報処理装置及び上記第2の情報処理装置において、一方向関数を演算した結果の最上位mビットを用いてデータP、データQ'、データQ及びデータP'を生成する請求の範囲第5 1項記載の情報処理方法。

5 3. 上記第1の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数R 1と上記生成した乱数S 1を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵K 1を生成すると共に、生成された暗号鍵K 1と受信した乱数R 2と上記生成した乱数S 2を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵K 2を生成し、

上記第2の情報処理装置は、自分が正当な機器であることを示す



情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵  $K_1'$  を生成すると共に、生成された暗号鍵  $K_1'$  と受信した乱数  $S_2$  と上記生成した乱数  $S_2$  を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵  $K_2'$  を生成する請求の範囲第 4 6 項記載の情報処理方法。

54. 上記第 1 の情報処理装置は、上記生成された暗号鍵  $K_1$  と受信した乱数  $R_2$  と上記生成した乱数  $S_2$  を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ  $P$  を上記第 2 の情報処理装置に送信し、

上記第 2 の情報処理装置は、上記生成された暗号鍵  $K_1'$  と受信した乱数  $S_2$  と上記生成した乱数  $R_2$  を連結した連結データに対して一方向関数を演算した結果を用いてデータ  $P'$  と受信したデータ  $P$  とが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ  $Q$  を上記第 1 の情報処理装置に送信し、

上記第 1 の情報処理装置は、自分が正当な機器であることを示す情報と受信した乱数  $R_1$  と上記生成した乱数  $S_1$  を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ  $Q'$  が受信したデータ  $Q$  と一致した場合には、暗号鍵  $K_2$  を生成する請求の範囲第 5 3 項記載の情報処理方法。

55. 伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースと、上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で暗号化して第 1 の伝

送モードで上記インターフェースを介して送信し、上記データに関する関連データを第2の暗号鍵で暗号化して第2の伝送モードで上記インターフェースを介して送信する送信制御手段とを備える情報処理装置。

56. 上記送信制御手段は、データ伝送に先立って、他の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する請求の範囲第55項記載の情報処理装置。

57. 上記送信制御手段は、音楽データを上記第1の伝送モードで伝送し、上記音楽データに関する関連データを第2の伝送モードで伝送する請求の範囲第55項記載の情報処理装置。

58. 上記インターフェースとしてIEEE(The International of Electrical and Electronics Engineers, Inc.)1394規格に準拠したインターフェースを有し、上記送信制御手段は、伝送帯域の保証が必要なデータをアイソクロナス(Isochronous)伝送モードで伝送し、上記データに関する関連データをアシンクロナス(Asynchronous)伝送モードで伝送する請求の範囲第55項記載の情報処理装置。

59. 上記送信制御手段は、データ伝送に先立って、他の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス(Asynchronous)伝送モードで実行する請求の範囲第58項記載の情報処理装置。

60. 上記送信制御手段は、2つの乱数を生成して他の情報処理装置に送信して、上記他の情報処理装置が生成した2つの乱数を受信し、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて第1の伝送モードで送信するデータを

暗号化するために使用する暗号鍵及び第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵を生成する請求の範囲第 55 項の情報処理装置。

61. 上記送信制御手段は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて生成したデータ P を上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ Q を受信し、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ Q' が受信したデータ Q と一致した場合には、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵を生成する請求の範囲第 60 項記載の情報処理装置。

62. 上記送信制御手段は、上記他の情報処理装置が生成した乱数 R2 を受信し、2 つの乱数 S1, S2 を生成して上記他の情報処理装置に送信するとともに、自分が正当な機器であることを示す情報と上記生成した乱数 S2 と受信した乱数 R2 とに基づいて生成したデータ P を上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数 S1 と生成した乱数 R1 とに基づいて生成したデータ Q を受信し、自分が正当な機器であることを示す情報と上記生成した乱数 S1 と受信した乱数 R1 とに基づいて生成したデータ Q' が受信したデータ Q と一致した場合には、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵 K1 及び上記第 2 の伝送モードで送

信するデータを暗号化するために使用する暗号鍵  $K_2$  を生成する請求の範囲第 6.1 項記載の情報処理装置。

63. 上記送信制御手段は、自分が正当な機器であることを示す情報と上記生成した乱数  $S_1$  と受信した乱数  $R_1$  を用いて一方向関数を演算した結果を用いて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_1$  を生成すると共に、自分が正当な機器であることを示す情報と上記生成した乱数  $S_2$  と受信した乱数  $R_2$  を用いて一方向関数を演算した結果を用いて、上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_2$  を生成する請求の範囲第 6.2 項記載の情報処理装置。

64. 上記送信制御手段は、自分が正当な機器であることを示す情報と上記生成した乱数  $S_2$  と受信した乱数  $R_2$  を用いて一方向関数を演算した結果を用いて生成したデータ  $P$  を上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  を用いて一方向関数を演算した結果を用いて生成したデータ  $Q$  を受信し、自分が正当な機器であることを示す情報と上記生成した乱数  $S_1$  と受信した乱数  $R_1$  を用いて一方向関数を演算した結果を用いて生成したデータ  $Q'$  が受信したデータ  $Q$  と一致した場合には、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_1$  及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵  $K_2$  を生成する請求の範囲第 6.3 項記載の情報処理装置。

65. 上記送信制御手段は、一方向関数を演算した結果の一部のビット値を用いて暗号鍵  $K_1$  及び暗号鍵  $K_2$  を生成する請求の範囲

第 6 3 項記載の情報処理装置。

6 6 . 上記送信制御手段は、一方向関数を演算した結果の一部のビット値を用いてデータ P 及びデータ Q' を生成する請求の範囲第 6 5 項記載の情報処理装置。

6 7 . 上記送信制御手段は、一方向関数を演算した結果の最下位 n ビットを用いて、暗号鍵 K 1 及び暗号鍵 K 2 を生成する請求の範囲第 6 5 項記載の情報処理装置。

6 8 . 上記送信制御手段は、一方向関数を演算した結果の最上位 m ビットを用いてデータ P 及びデータ Q' を生成する請求の範囲第 6 7 項記載の情報処理装置。

6 9 . 上記送信制御手段は、自分が正当な機器であることを示す情報と上記生成した乱数 S 1 と受信した乱数 R 1 を連結した連結データに対して一方向関数を演算した結果を用いて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵 K 1 を生成すると共に、自分が正当な機器であることを示す情報と上記生成した乱数 S 2 と受信した乱数 R 2 を連結した連結データに対して一方向関数を演算した結果を用いて、上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵 K 2 を生成する請求の範囲第 6 2 項記載の情報処理装置。

7 0 . 上記送信制御手段は、自分が正当な機器であることを示す情報と上記生成した乱数 S 2 と受信した乱数 R 2 を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ P を上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数 S 1 と上記生成した乱数 R 1 を連結した連結データに対して一方向関数を演算した

結果を用いて生成したデータ Q を受信し、自分が正当な機器であることを示す情報と上記生成した乱数 S 1 と受信した乱数 R 1 を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ Q' が受信したデータ Q と一致した場合には、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵 K 1 及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵 K 2 を生成する請求の範囲第 6 9 項記載の情報処理装置。

7 1. 上記送信制御手段は、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成し、生成された暗号鍵と上記生成した乱数と受信した乱数とに基づいて、他方の伝送モードの暗号鍵を生成する請求の範囲第 6 0 項記載の情報処理装置。

7 2. 上記送信制御手段は、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成すると共に、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータ P を上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ Q を受信し、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数

とに基づいて生成したデータ  $Q'$  が受信したデータ  $Q$  と一致した場合には、既に生成されている伝送モード用の暗号鍵と受信した乱数と上記生成した乱数とに基づいて、上記第 1 の伝送モード及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵を生成する請求の範囲第 7 1 項記載の情報処理装置。

7 3. 上記送信制御手段は、上記他の情報処理装置が生成した 2 つの乱数  $R_1$ ,  $R_2$  を受信し、2 つの乱数  $S_1$ ,  $S_2$  を生成して上記他の情報処理装置に送信するとともに、自分が正当な機器であることを示す情報と受信した乱数  $R_1$  と上記生成した乱数  $S_1$  とに基づいて、上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵  $K_1$  を生成すると共に、上記生成された暗号鍵  $K_1$  と受信した乱数  $R_2$  と上記生成した乱数  $S_2$  とに基づいて生成したデータ  $P$  を上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  とに基づいて生成したデータ  $Q$  を受信し、自分が正当な機器であることを示す情報と受信した乱数  $R_1$  と上記生成した乱数  $S_1$  とに基づいて生成したデータ  $Q'$  が受信したデータ  $Q$  と一致した場合には、既に生成されている伝送モード用の暗号鍵  $K_1$  と受信した乱数  $R_2$  と上記生成した乱数  $S_2$  とに基づいて、上記第 1 の伝送モード及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵  $K_2$  を生成する請求の範囲第 7 2 項記載の情報処理装置。

74. 上記送信制御手段は、自分が正当な機器であることを示す情報と受信した乱数R1と上記生成した乱数S1とを用いて一方向関数を演算した結果を用いて暗号鍵K1を生成すると共に、生成された暗号鍵K1と受信した乱数R2と上記生成した乱数S2とを用いて一方向関数を演算した結果を用いて暗号鍵K2を生成する請求の範囲第73項記載の情報処理装置。

75. 上記送信制御手段は、上記生成された暗号鍵K1と受信した乱数R2と上記生成した乱数S2とを用いて一方向関数を演算した結果を用いて生成したデータPを上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数S1と上記生成した乱数R1とを用いて一方向関数を演算した結果を用いて生成したデータQを受信し、自分が正当な機器であることを示す情報と受信した乱数R1と上記生成した乱数S1とを用いて一方向関数を演算した結果を用いて生成したデータQ'が受信したデータQと一致した場合には、暗号鍵K2を生成する請求の範囲第74項記載の情報処理装置。

76. 上記送信制御手段は、一方向関数を演算した結果の一部のビット値を用いて暗号鍵K1及び暗号鍵K2を生成する請求の範囲第74項記載の情報処理装置。

77. 上記送信制御手段は、一方向関数を演算した結果の一部のビット値を用いてデータP及びデータQ'を生成する請求の範囲第76項記載の情報処理装置。

78. 上記送信制御手段は、一方向関数を演算した結果の最下位nビットを用いて、暗号鍵K1及び暗号鍵K2を生成する請求の範囲第76項記載の情報処理装置。



79. 上記送信制御手段は、一方向関数を演算した結果の最上位  $m$  ビットを用いてデータ  $P$  及びデータ  $Q'$  を生成する請求の範囲第 78 項記載の情報処理装置。

80. 上記送信制御手段は、自分が正当な機器であることを示す情報と受信した乱数  $R_1$  と上記生成した乱数  $S_1$  を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵  $K_1$  を生成すると共に、生成された暗号鍵  $K_1$  と受信した乱数  $R_2$  と上記生成した乱数  $S_2$  を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵  $K_2$  を生成する請求の範囲第 73 項記載の情報処理装置。

81. 上記送信制御手段は、上記生成された暗号鍵  $K_1$  と受信した乱数  $R_2$  と上記生成した乱数  $S_2$  を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ  $P$  を上記他の情報処理装置に送信して、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ  $Q$  を受信し、自分が正当な機器であることを示す情報と受信した乱数  $R_1$  と上記生成した乱数  $S_1$  を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ  $Q'$  が受信したデータ  $Q$  と一致した場合には、暗号鍵  $K_2$  を生成する請求の範囲第 80 項記載の情報処理装置。

82. 伝送帯域が保証された第 1 の伝送モードと伝送帯域が保証されていない第 2 の伝送モードを持つインターフェースと、上記インターフェースを介して第 1 の伝送モードで受信される上記伝送帯域の保証が必要なデータを第 1 の暗号鍵で復号し、上記インターフ

エースを介して第 2 の伝送モードで受信される上記関連データを第 2 の暗号鍵で復号する受信制御手段とを備える情報処理装置。

8 3. 上記受信制御手段は、データ伝送に先立って、他の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する請求の範囲第 8 2 項記載の情報処理装置。

8 4. 上記受信制御手段は、音楽データを上記第 1 の伝送モードで受信し、上記音楽データに関する関連データを第 2 の伝送モードで受信する請求の範囲第 8 2 項記載の情報処理装置。

8 5. 上記インターフェースとして I E E E (The International of Electrical and Electronics Engineers, Inc.) 1 3 9 4 規格に準拠したインターフェースを有し、上記受信制御手段は、伝送帯域の保証が必要なデータをアイソクロナス (Isochronous) 伝送モードで受信し、上記データに関する関連データをアシンクロナス (Asynchronous) 伝送モードで受信する請求の範囲第 8 2 項記載の情報処理装置。

8 6. 上記受信制御手段は、データ伝送に先立って、上記他の情報処理装置との間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス (Asynchronous) 伝送モードで実行する請求の範囲第 8 5 項記載の情報処理装置。

8 7. 上記受信制御手段は、2 つの乱数を生成して他の情報処理装置に送信して、上記他の情報処理装置が生成した 2 つの乱数を受信し、自分が正当な機器であることを示す情報と上記生成した乱数と受信した乱数とに基づいて第 1 の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵を生成する請求の範

図第 8 2 項の情報処理装置。

8 8. 上記受信制御手段は、上記他の情報処理装置が自分が正当な機器であることを示す情報と生成した乱数と受信した乱数とに基づいて生成したデータ P を受信して、

自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ Q を上記他の情報処理装置に送信し、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ P' が受信したデータ P と一致した場合には、上記第 1 の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵を生成する請求の範囲第 8 7 項記載の情報処理装置。

8 9. 上記受信制御手段は、2つの乱数 R 1, R 2 を生成して他の情報処理装置に送信して、上記他の情報処理装置が生成した2つの乱数 S 1, S 2 を受信するとともに、上記他の情報処理装置が自分が正当な機器であることを示す情報と上記生成した乱数 S 2 と受信した乱数 R 2 とに基づいて生成したデータ P を受信し、自分が正当な機器であることを示す情報と受信した乱数 S 1 と上記生成した乱数 R 1 とに基づいて生成したデータ Q を上記他の情報処理装置に送信するとともに、自分が正当な機器であることを示す情報と受信した乱数 S 2 と上記生成した乱数 R 2 とに基づいて生成したデータ P' が受信したデータ P と一致した場合には、上記第 1 の伝送モードで送信されるデータを復号するために使用する暗号鍵 K' 1 及び上記第 2 の伝送モードで送信されるデータを復号するために使用する暗号鍵 K' 2 を生成する請求の範囲第 8 8 項記載の情報処理装置。

90. 上記受信制御手段は、自分が正当な機器であることを示す情報と受信した乱数S1と上記生成した乱数R1を用いて一方向関数を演算した結果を用いて、上記第1の伝送モードで送信されるデータを復号するために使用する暗号鍵K'1を生成すると共に、自分が正当な機器であることを示す情報と受信した乱数S2と上記生成した乱数R2を用いて一方向関数を演算した結果を用いて、上記第2の伝送モードで送信されるデータを復号するために使用する暗号鍵K'2を生成する請求の範囲第89項記載の情報処理装置。

91. 上記受信制御手段は、上記他の情報処理装置が自分が正当な機器であることを示す情報と上記生成した乱数S2と受信した乱数R2を用いて一方向関数を演算した結果を用いて生成したデータPを受信し、自分が正当な機器であることを示す情報と受信した乱数S1と上記生成した乱数R1を用いて一方向関数を演算した結果を用いて生成したデータQを上記他の情報処理装置に送信し、自分が正当な機器であることを示す情報と受信した乱数S2と上記生成した乱数R2を用いて一方向関数を演算した結果を用いて生成したデータP'が受信したデータPと一致した場合には、上記第1の伝送モードで送信されるデータを復号するために使用する暗号鍵K'1及び上記第2の伝送モードで送信されるデータを復号するために使用する暗号鍵K'2を生成する請求の範囲第90項記載の情報処理装置。

92. 上記受信制御手段は、一方向関数を演算した結果の一部のビット値を用いて暗号鍵K'1及び暗号鍵K'2を生成する請求の範囲第90項記載の情報処理装置。

93. 上記受信制御手段は、一方向関数を演算した結果の一部の

ビット値を用いてデータ Q 及びデータ P' を生成する請求の範囲第 9 2 項記載の情報処理装置。

9 4. 上記受信制御手段は、一方向関数を演算した結果の最下位 n ビットを用いて、暗号鍵 K' 1 及び暗号鍵 K' 2 を生成する請求の範囲第 9 2 項記載の情報処理装置。

9 5. 上記受信制御手段は、一方向関数を演算した結果の最上位 m ビットを用いてデータ Q 及びデータ P' を生成する請求の範囲第 9 4 項記載の情報処理装置。

9 6. 上記受信制御手段は、自分が正当な機器であることを示す情報と受信した乱数 S 1 と上記生成した乱数 R 1 を連結した連結データに対して一方向関数を演算した結果を用いて、上記第 1 の伝送モードで送信されるデータを復号するために使用する暗号鍵 K' 1 を生成すると共に、自分が正当な機器であることを示す情報と受信した乱数 S 2 と上記生成した乱数 R 2 を連結した連結データに対して一方向関数を演算した結果を用いて、上記第 2 の伝送モードで送信されるデータを復号するために使用する暗号鍵 K' 2 を生成する請求の範囲第 8 9 項記載の情報処理装置。

9 7. 上記受信制御手段は、上記他の情報処理装置が自分が正当な機器であることを示す情報と上記生成した乱数 S 2 と受信した乱数 R 2 を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ P を受信し、自分が正当な機器であることを示す情報と受信した乱数 S 1 と上記生成した乱数 R 1 を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ Q を上記他の情報処理装置に送信し、自分が正当な機器であることを示す情報と受信した乱数 S 2 と上記生成した乱数 R 2 を連結し

た連結データに対して一方向関数を演算した結果を用いて生成したデータ P' が受信したデータ P と一致した場合には、上記第 1 の伝送モードで送信されるデータを復号するために使用する暗号鍵 K' 1

及び上記第 2 の伝送モードで送信されるデータを復号するために使用する暗号鍵 K' 2 を生成する請求の範囲第 9 6 項記載の情報処理装置。

9 8. 上記受信制御手段は、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて上記第 1 の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第 2 の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵を生成し、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータ P を受信し、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて、上記第 1 の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のいずれか一方の暗号鍵を生成すると共に、上記生成された暗号鍵と受信した乱数と上記生成した乱数とに基づいて生成したデータ P' が受信したデータ P とが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数と上記生成した乱数とに基づいて生成したデータ Q を上記他の情報処理装置に送信すると共に、既に生成されている伝送モード用の暗号鍵と受信した乱数と上記生成した乱数とに基づいて、上記第 1 の伝送モード及び上記第 2 の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝

送モードの暗号鍵を生成する請求の範囲第 8 7 項記載の情報処理装置。

9 9. 上記受信制御手段は、2つの乱数 $R_1$ 、 $R_2$ を生成して他の情報処理装置に送信し、上記他の情報処理装置が生成した2つの乱数 $S_1$ 、 $S_2$ を受信するとともに、上記他の情報処理装置が自分が正当な機器であることを示す情報と受信した乱数 $R_1$ と上記生成した乱数 $S_1$ とに基づいて、上記第1の伝送モードで送信するデータを暗号化するために使用する暗号鍵及び上記第2の伝送モードで送信するデータを暗号化するために使用する暗号鍵のいずれか一方の暗号鍵 $K_1$ を生成すると共に、上記生成された暗号鍵 $K_1$ と受信した乱数 $R_2$ と上記生成した乱数 $S_2$ とに基づいて生成したデータ $P$ を受信し、自分が正当な機器であることを示す情報と受信した乱数 $S_1$ と上記生成した乱数 $R_1$ とに基づいて、上記第1の伝送モードで送られてくるデータを復号するために使用する暗号鍵及び上記第2の伝送モードで送られてくるデータを復号するために使用する暗号鍵のいずれか一方の暗号鍵 $K_1'$ を生成すると共に、上記生成された暗号鍵 $K_1'$ と受信した乱数 $S_2$ と上記生成した乱数 $R_2$ とに基づいて生成したデータ $P'$ と受信したデータ $P$ とが一致するかどうかを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数 $S_1$ と上記生成した乱数 $R_1$ とに基づいて生成したデータ $Q$ を上記他の情報処理装置に送信すると共に、既に生成されている伝送モード用の暗号鍵 $K_1'$ と受信した乱数 $S_2$ と上記生成した乱数 $S_2$ とに基づいて、上記第1の伝送モード及び上記第2の伝送モードで送られてくるデータを復号するために使用する暗号鍵のうちまだ生成していない伝送モードの暗号鍵 $K_2'$ を生

成する請求の範囲第 9 8 項記載の情報処理装置。

1 0 0. 上記受信制御手段は、自分が正当な機器であることを示す情報と受信した乱数 S 1 と上記生成した乱数 R 1 とを用いて一方向関数を演算した結果を用いて暗号鍵 K 1' を生成すると共に、生成された暗号鍵 K 1' と受信した乱数 S 2 と上記生成した乱数 S 2 とを用いて一方向関数を演算した結果を用いて暗号鍵 K 2' を生成する請求の範囲第 9 9 項記載の情報処理装置。

1 0 1. 上記受信制御手段は、上記他の情報処理装置が上記生成された暗号鍵 K 1 と受信した乱数 R 2 と上記生成した乱数 S 2 とを用いて一方向関数を演算した結果を用いて生成したデータ P を受信し、上記生成された暗号鍵 K 1' と受信した乱数 S 2 と上記生成した乱数 R 2 とを用いて一方向関数を演算した結果を用いてデータ P' と受信したデータ P とが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数 S 1 と上記生成した乱数 R 1 とを用いて一方向関数を演算した結果を用いて生成したデータ Q を上記他の情報処理装置に送信する請求の範囲第 1 0 0 項記載の情報処理装置。

1 0 2. 上記受信制御手段は、一方向関数を演算した結果の一部のビット値を用いて暗号鍵 K' 1 及び暗号鍵 K' 2 を生成する請求の範囲第 1 0 0 項記載の情報処理装置。

1 0 3. 上記受信制御手段は、一方向関数を演算した結果の一部のビット値を用いてデータ Q 及びデータ P' を生成する請求の範囲第 1 0 2 項記載の情報処理装置。

1 0 4. 上記受信制御手段は、一方向関数を演算した結果の最下位 n ビットを用いて、暗号鍵 K' 1 及び暗号鍵 K' 2 を生成する請



求の範囲第 1 0 2 項記載の情報処理装置。

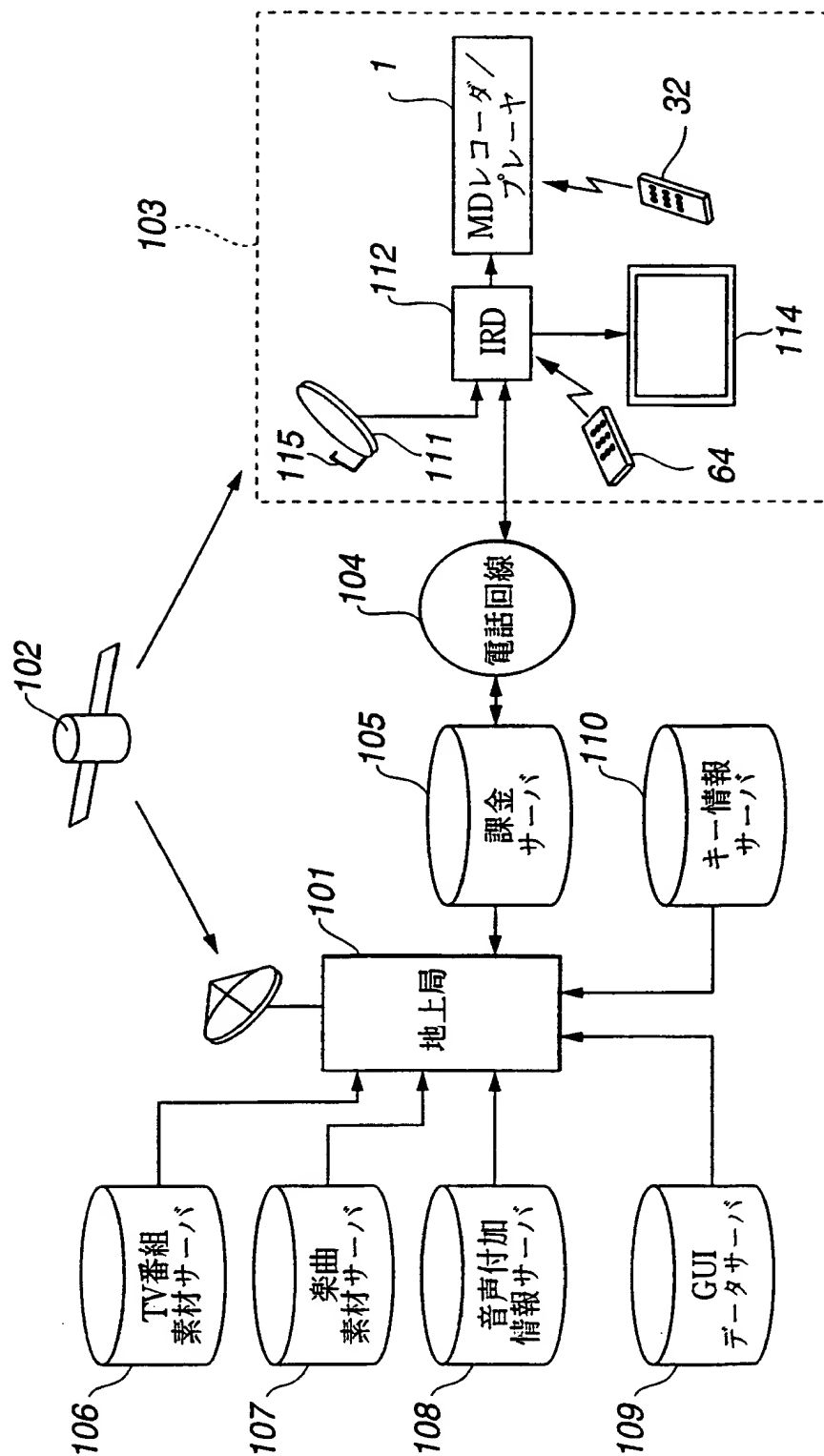
1 0 5. 上記受信制御手段は、一方向関数を演算した結果の最上位  $m$  ビットを用いてデータ  $Q$  及びデータ  $P'$  を生成する請求の範囲第 1 0 4 項記載の情報処理装置。

1 0 6. 上記受信制御手段は、自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵  $K_1'$  を生成すると共に、生成された暗号鍵  $K_1'$  と受信した乱数  $S_2$  と上記生成した乱数  $S_2$  を連結した連結データに対して一方向関数を演算した結果を用いて暗号鍵  $K_2'$  を生成する請求の範囲第 9 9 項記載の情報処理装置。

1 0 7. 上記受信制御手段は、上記他の情報処理装置が上記生成された暗号鍵  $K_1$  と受信した乱数  $R_2$  と上記生成した乱数  $S_2$  を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ  $P$  を受信し、上記生成された暗号鍵  $K_1'$  と受信した乱数  $S_2$  と上記生成した乱数  $R_2$  を連結した連結データに対して一方向関数を演算した結果を用いてデータ  $P'$  と受信したデータ  $P$  とが一致するか否かを検証し、一致した場合には、自分が正当な機器であることを示す情報と受信した乱数  $S_1$  と上記生成した乱数  $R_1$  を連結した連結データに対して一方向関数を演算した結果を用いて生成したデータ  $Q$  を上記他の情報処理装置に送信する請求の範囲第 1 0 6 項記載の情報処理装置。

**THIS PAGE BLANK (USPTO)**

**1/16**



**FIG. 1**

**THIS PAGE BLANK (USPTO)**

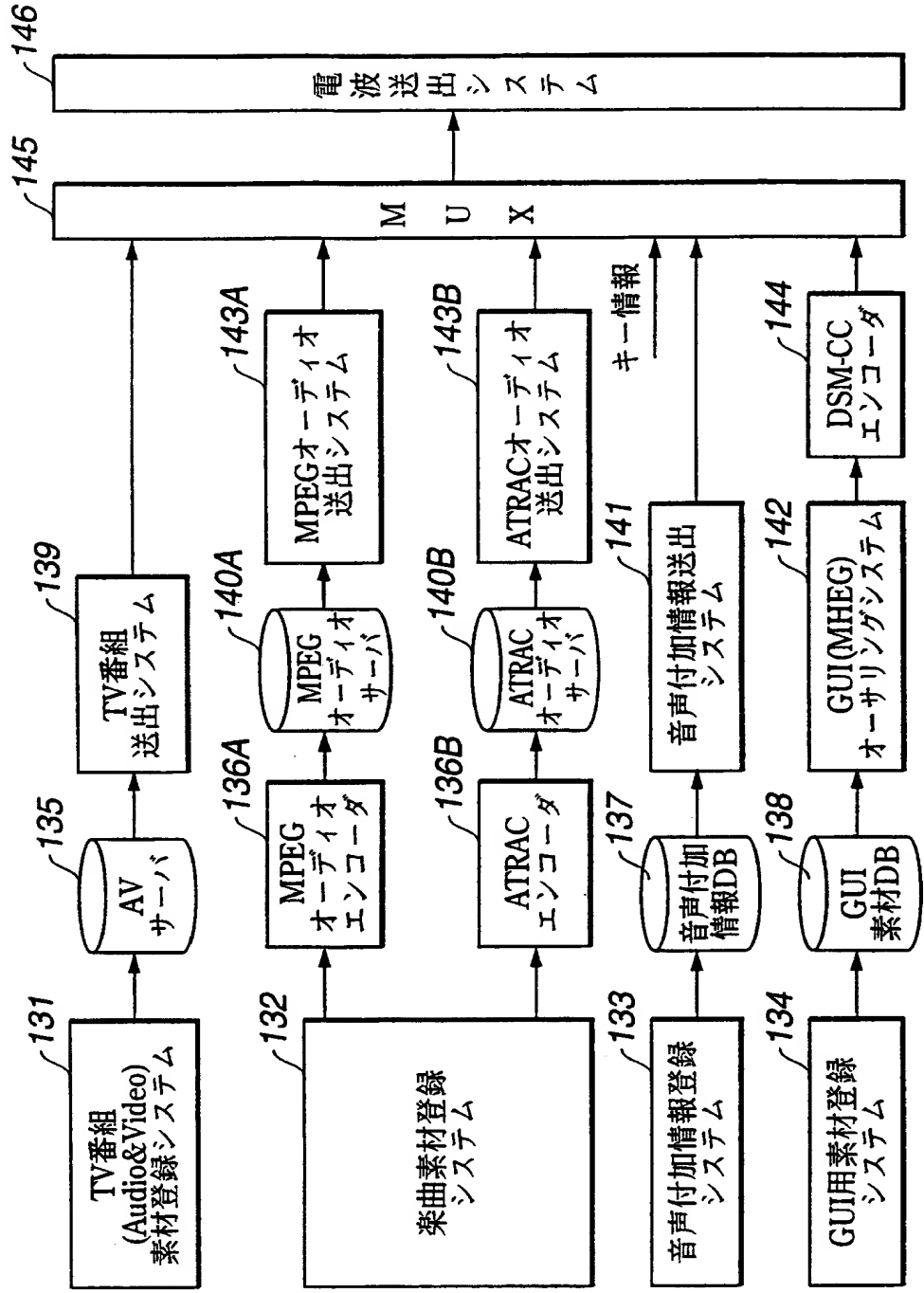


FIG.2

**THIS PAGE BLANK (USPTO)**

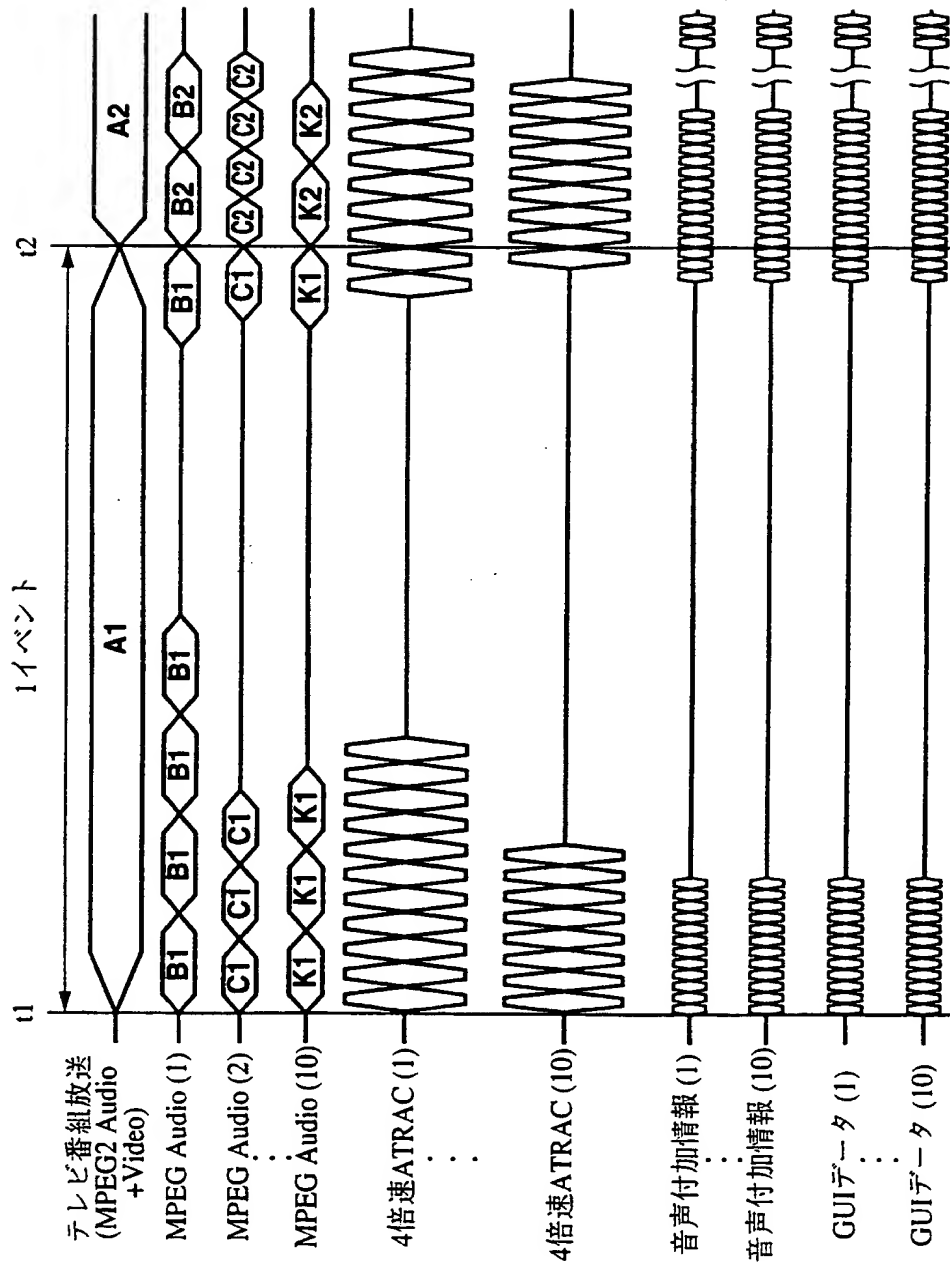
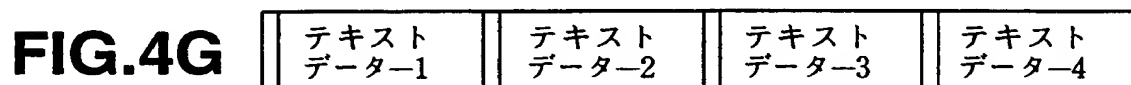


FIG.3

**THIS PAGE BLANK (USPTO)**



4/16



**THIS PAGE BLANK (USPTO)**

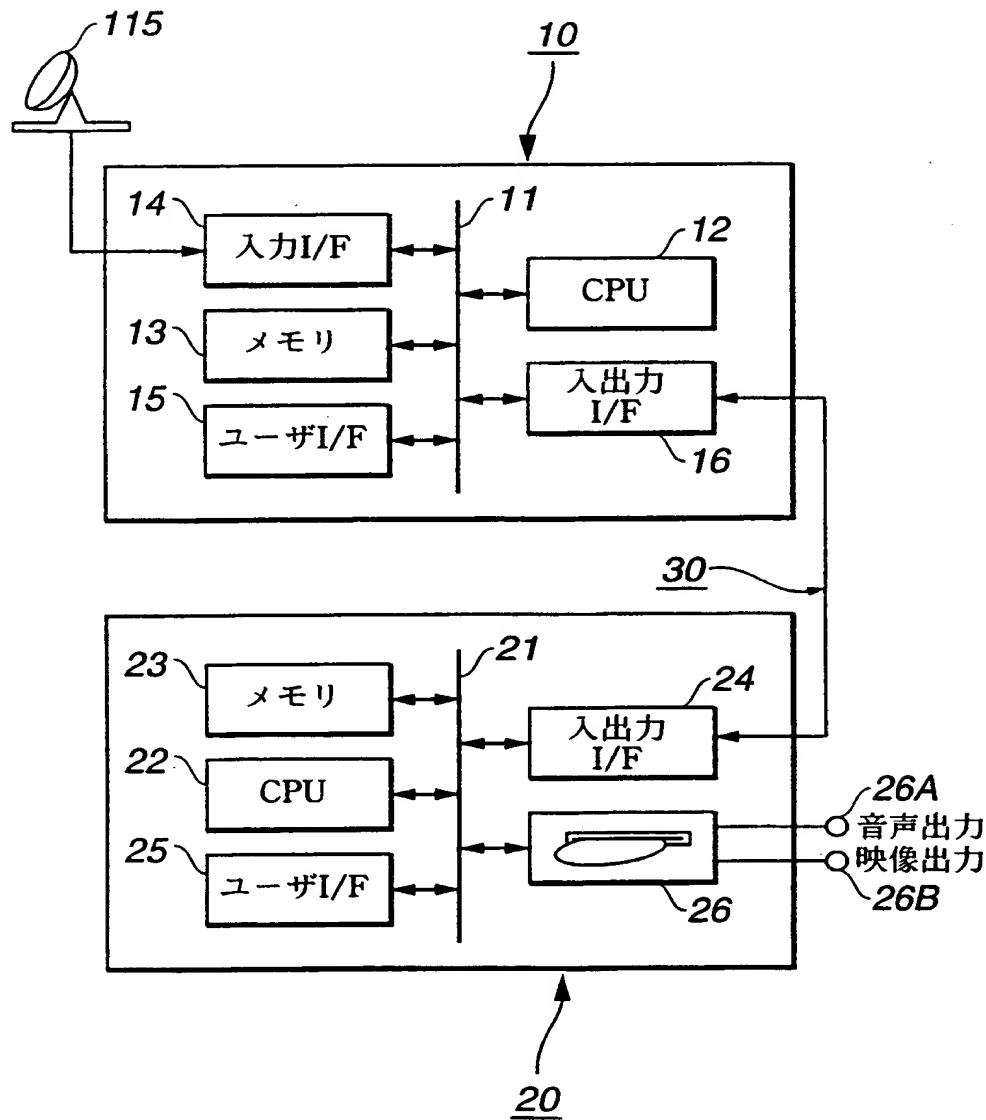
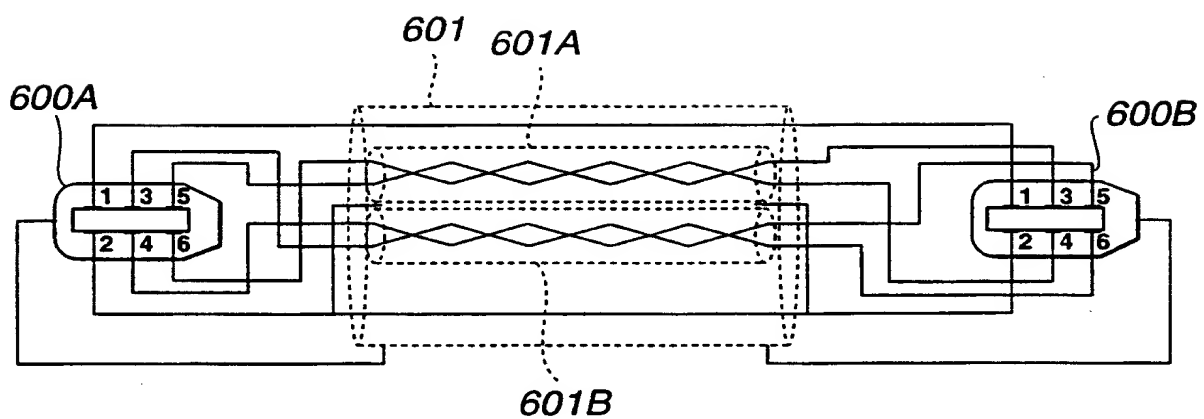


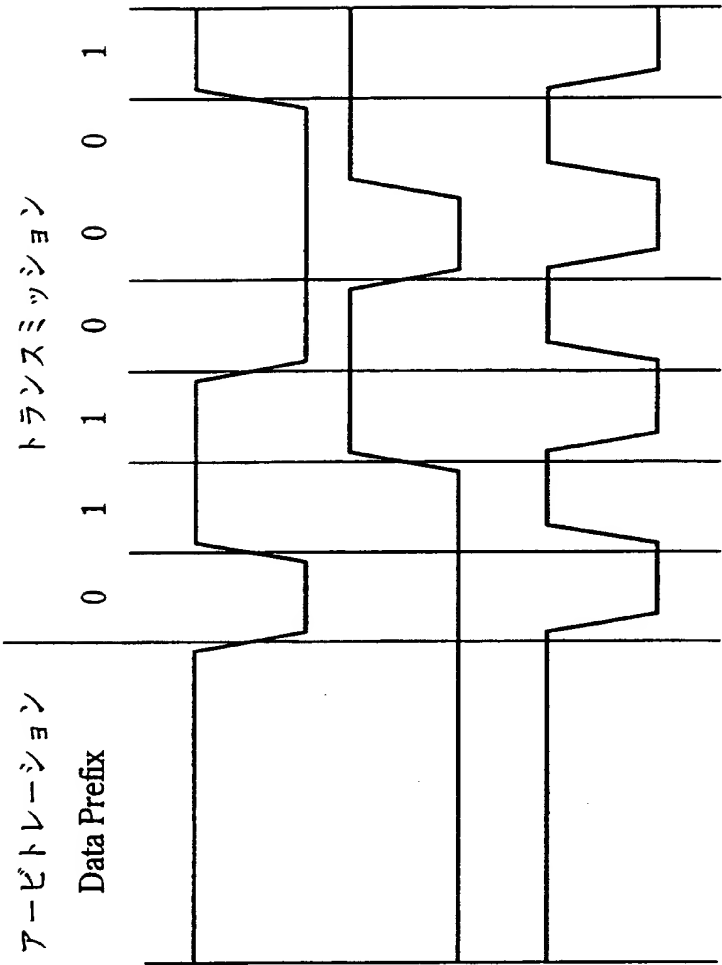
FIG.5

**THIS PAGE BLANK (USPTO)**

6/16

**FIG.6**

**THIS PAGE BLANK (USPTO)**



データ信号  
(TPBout-TPAin)

ストロブ信号  
(TPAout-TPBin)

伝送クロック  
(Data^Strobe)

FIG.7A

FIG.7B

FIG.7C

**THIS PAGE BLANK (USPTO)**



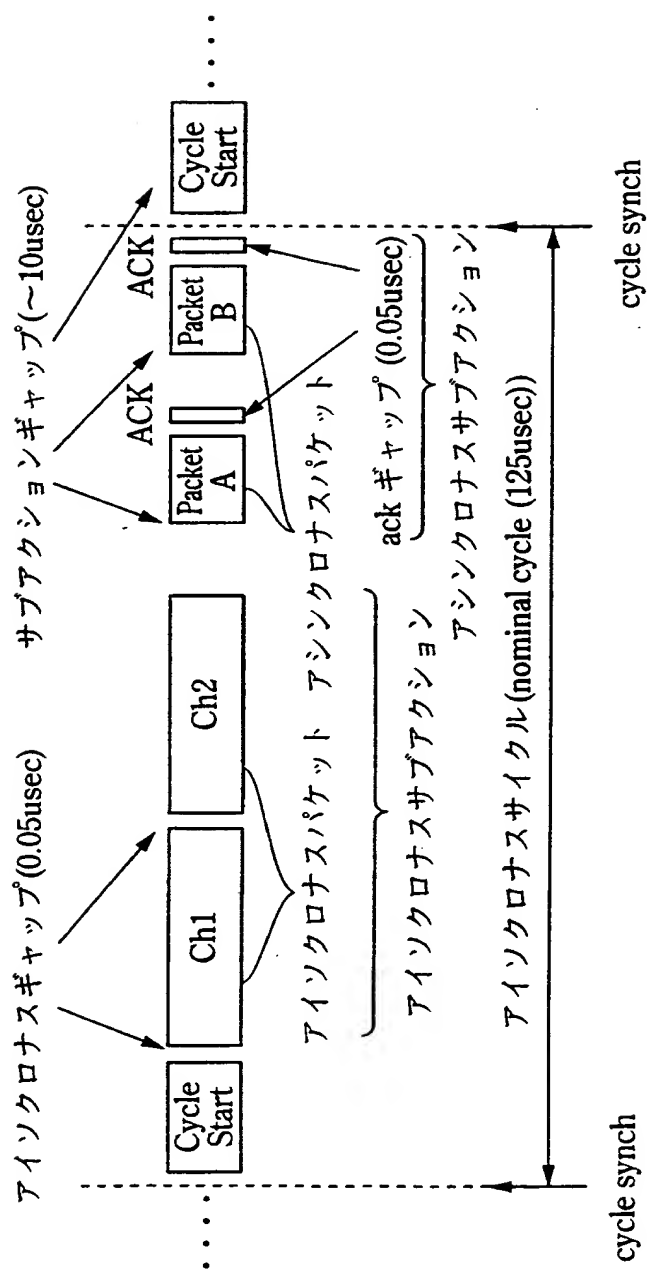
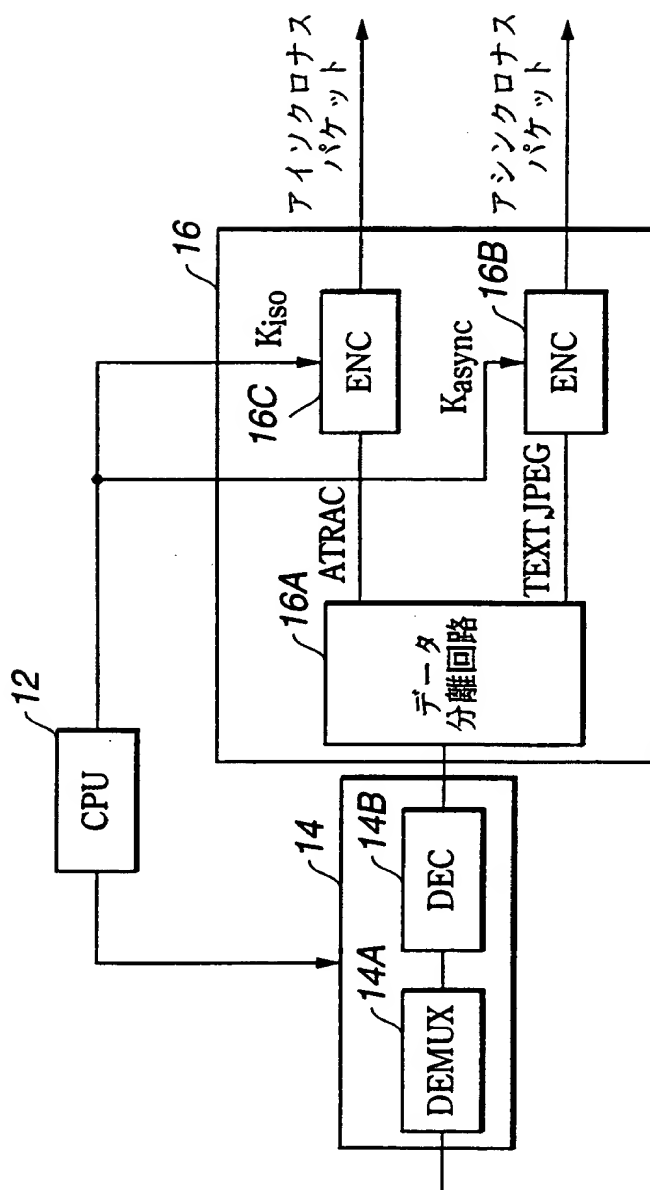


FIG.8

**THIS PAGE BLANK (USPTO)**



**FIG. 9**

**THIS PAGE BLANK (USPTO)**

10/16

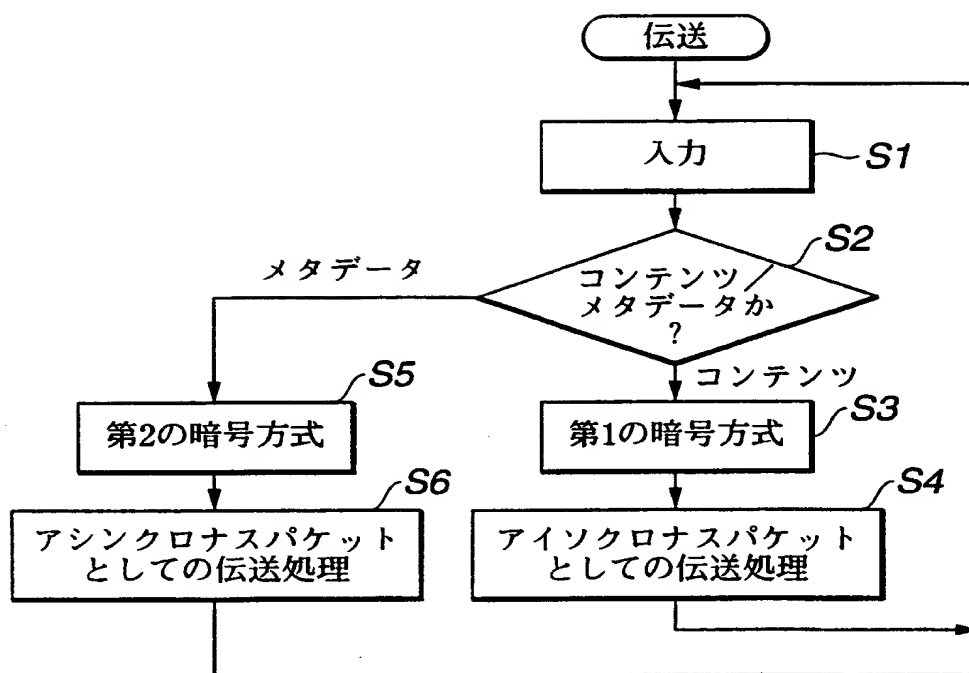


FIG.10

**THIS PAGE BLANK (USPTO)**



**THIS PAGE BLANK (USPTO)**



12/16

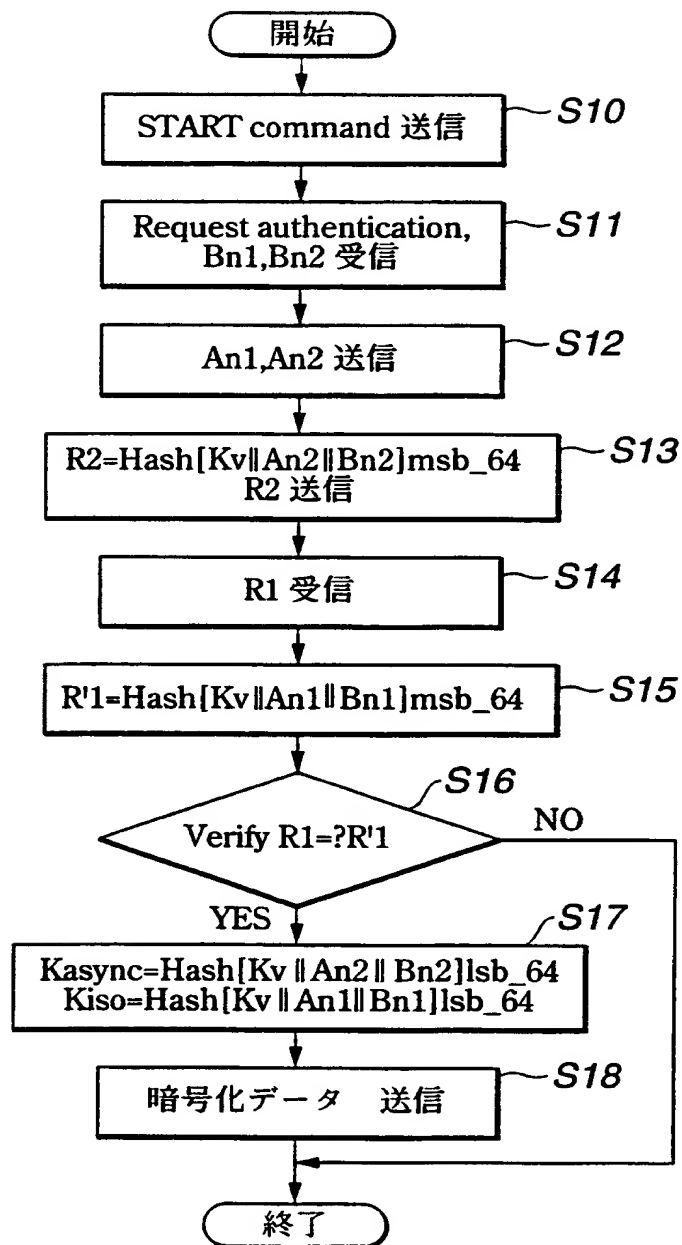


FIG.12

**THIS PAGE BLANK (USPTO)**

13/16

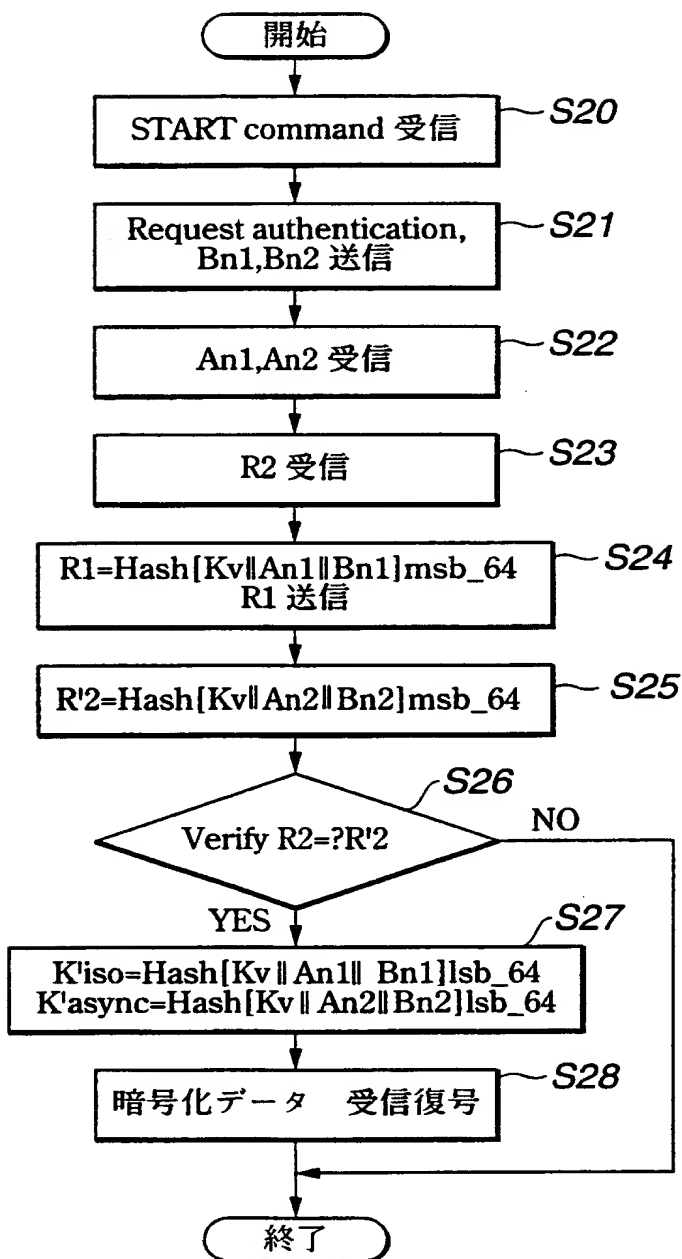


FIG.13

**THIS PAGE BLANK (USPTO)**

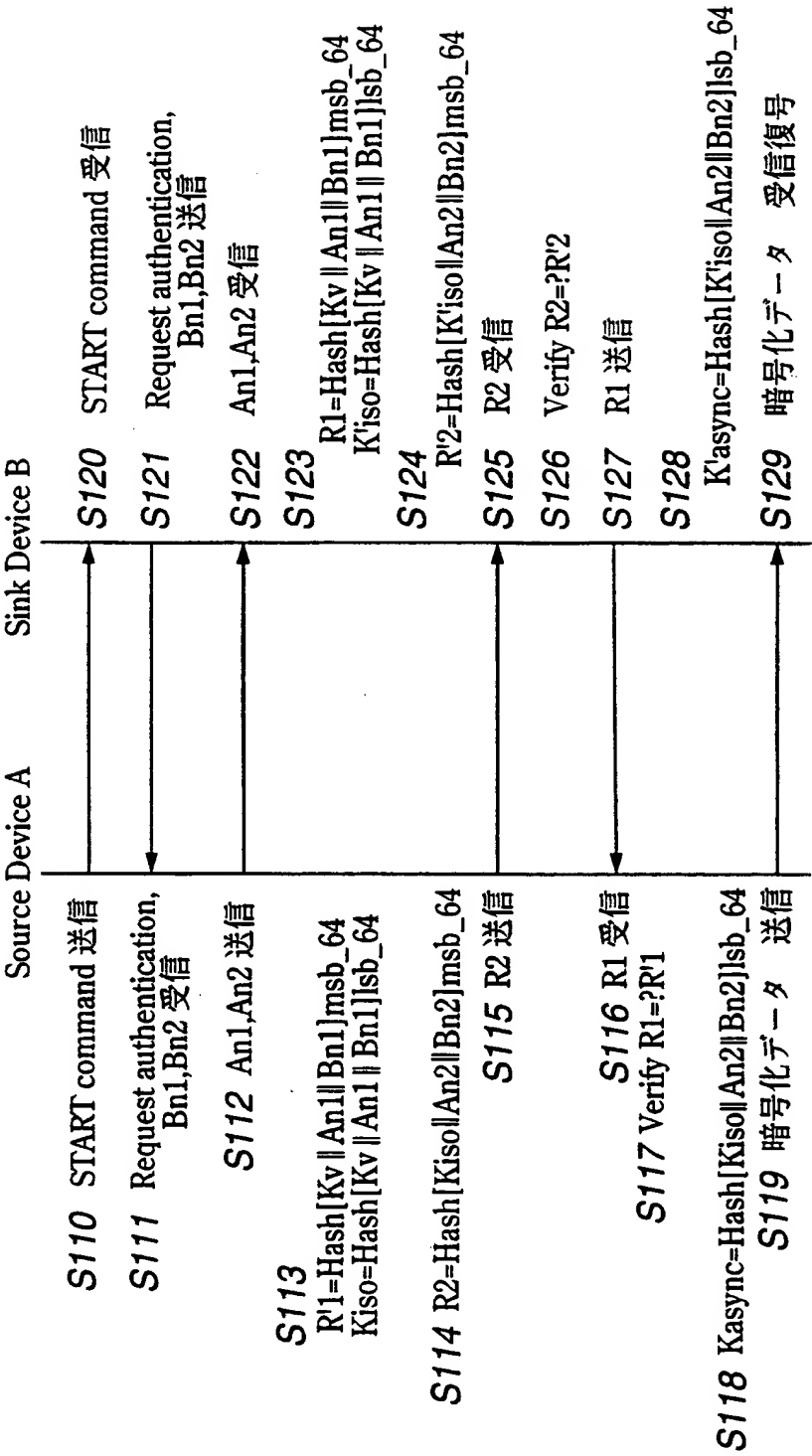


FIG.14

**THIS PAGE BLANK (USPTO)**

15/16

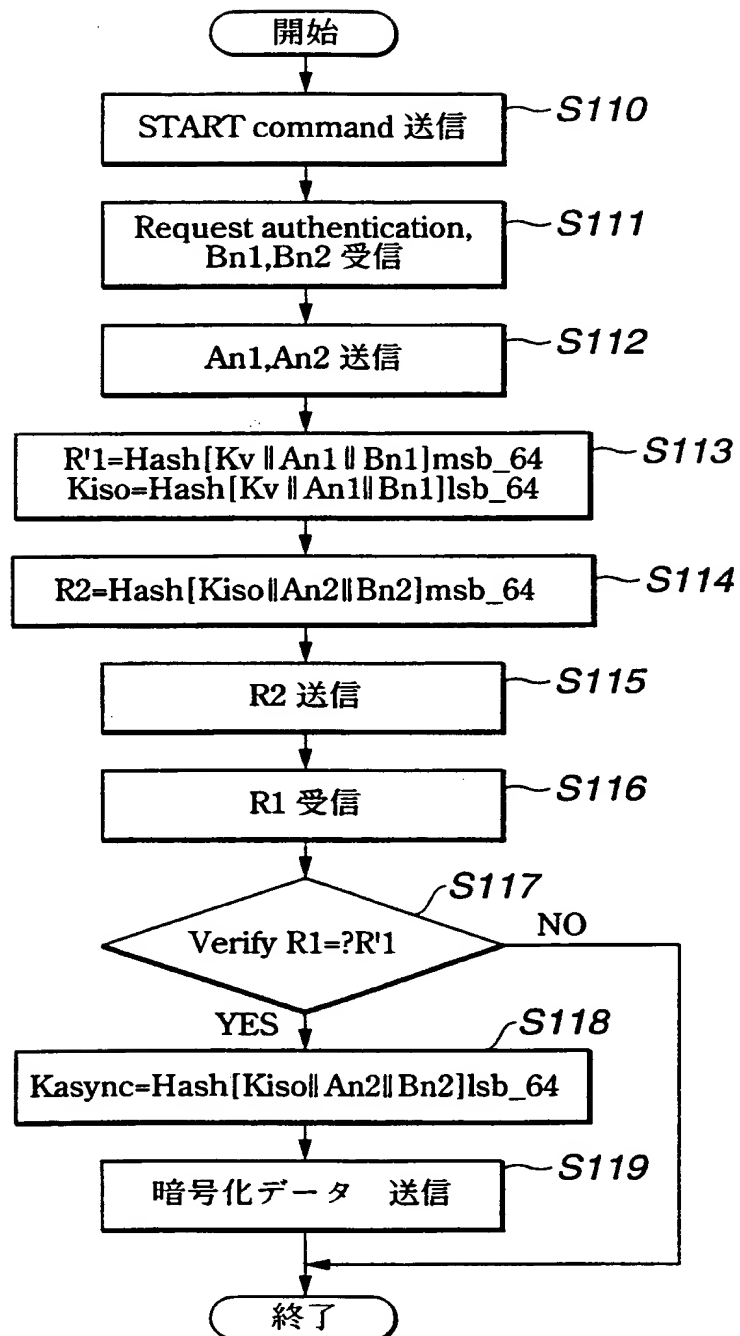


FIG.15





16/16

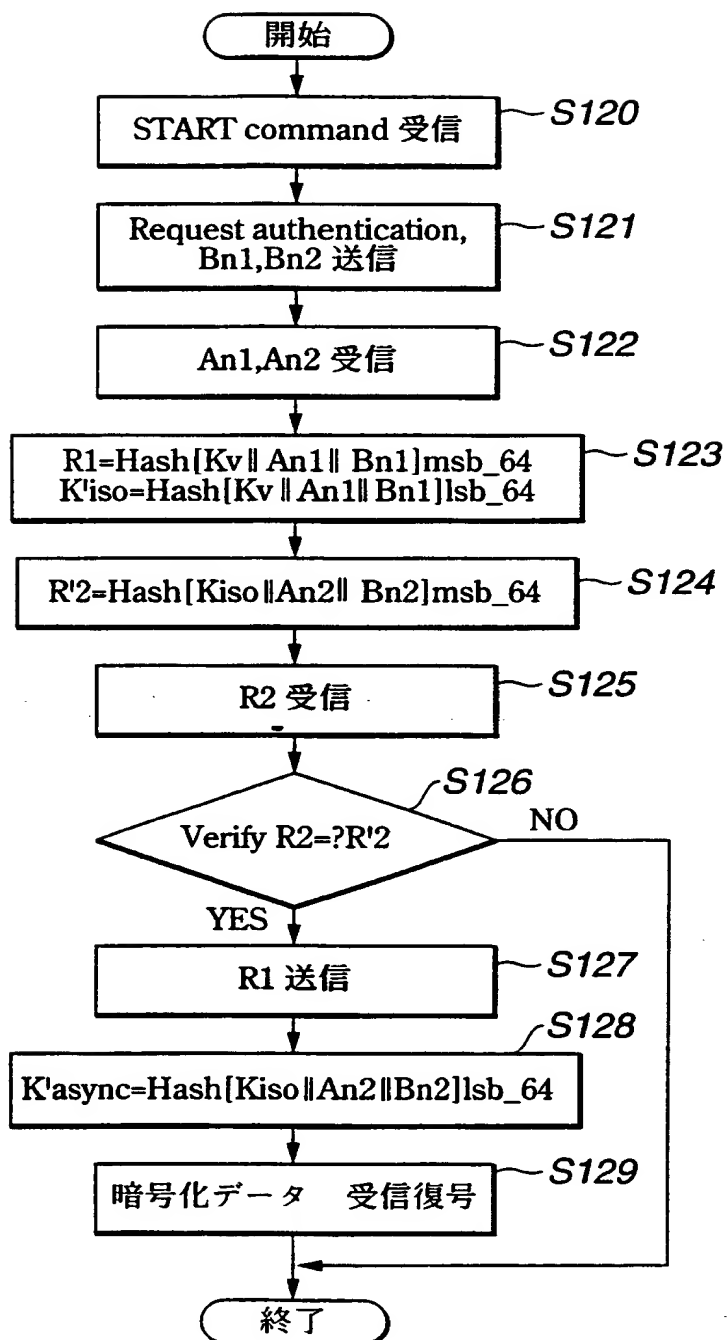


FIG16

**THIS PAGE BLANK (USPTO)**

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02353

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> H04L 9/08 H04L 9/32 H04L 12/28 H04H1/00  
H04N 7/167

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G09C 1/00 - 5/00 H04K 1/00 - 3/00 H04L 9/00 H04L 12/00 G11B 20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST File (JOIS)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 11-53264, A (Sony Corporation), 26 February, 1999 (26.02.99), especially see Par. No. [0218], Fig. 37	1-17, 28-44, 55-71, 82-97
A	& EP, 874300, A & KR, 98081632, A & CN, 1202659, A	18-27, 45-54, 72-81, 98-107
Y	JP, 10-224402, A (Toshiba Corporation), 21 August, 1998 (21.08.98), especially see Par. No. [0044], (Family: none)	1-17, 28-44, 55-71, 82-97
A		18-27, 45-54, 72-81, 98-107
Y	JP, 11-27315, A (Sanyo Electric Co., Ltd.), 29 January, 1999 (29.01.99), especially see Par. No. [0003], (Family: none)	3, 30, 57, 84
Y	JP, 10-21645, A (Sony Corporation), 23 January, 1998 (23.01.98), especially see Par. Nos. [0011] to [0012], (Family: none)	3, 30, 57, 84
Y	JP, 10-51439, A (Matsushita Electric Ind. Co., Ltd.), 20 February, 1998 (20.02.98),	6, 33, 60, 87

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search  
16 June, 2000 (16.06.00)

Date of mailing of the international search report  
04 July, 2000 (04.07.00)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02353

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	especially see Fig.3 & EP, 809379, A & TW, 333630, A & KR, 97076418, A	
Y	JP, 10-210023, A (Oki Electric Industry Co., Ltd.), 07 August, 1998 (07.08.98),	7-16, 34-43, 61-70, 88-97
A	especially see Fig.2, Par. No.[0138], (Family: none)	18-27, 45-54, 72-81, 98-107
Y	Hideki Tsubakiyama and Keiichiro Koga, "Security for Information Data Broadcasting System with Conditional-Access Control," 1993 Conference Record. IEEE GLOBECOM, Vol.1, (1993), pp.164-170, especially see Fig.3, Fig.4	9,11,13,15, 17,36,38,40, 42,44,63,65, 67,69,71,90, 92,94,96
A		18-27,45-54, 72-81,98-107
A	JP, 10-303945, A (Sony Corporation), 13 November, 1998 (13.11.98) & EP, 874503, A & KR, 98081633, A	2-5,29-32, 56-59,83-86
A	JP, 10-224763, A (Matsushita Electric Ind. Co., Ltd.), 21 August, 1998 (21.08.98) & EP, 858183, A & KR, 98071098, A	1-5,28-32, 55-59,82-86
A	Masanori Suzuki et al. "Eizou Kaigi System you Kosoku Serial Bus (IEEE 1394) Tsushin Houshiki" Joho Shori Gakkai Hokoku, Vol.96, No.12, (1996), pp.215-220 (96-DPS-74)	3,4,30,31, 57,58,84,85
A	JP, 9-74408, A (Nippon Telegr. & Teleph. Corp. <NTT>), 18 March, 1997 (18.03.97) (Family: none)	6-27,33-54, 60-81,87-107
A	JP, 7-264668, A (Kokusai Denshin Denwa Co., Ltd. (KDD), 13 October, 1995 (13.10.95) & EP, 673178, A & US, 5596641, A	7-16,18-27, 34-43,45-54, 61-70,72-81, 88-107

## 国際調査報告

国際出願番号 PCT/JP00/02353

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl<sup>7</sup> H04L 9/08 H04L 9/32 H04L 12/28 H04H1/00  
H04N 7/167

## B. 調査を行った分野

## 調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl<sup>7</sup> G09C 1/00 - 5/00 H04K 1/00 - 3/00 H04L 9/00  
H04L 12/00 G11B 20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用了電子データベース (データベースの名称、調査に使用した用語)  
JICSTファイル (JOIS)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	J P, 11-53264, A (ソニー株式会社) 26. 2月. 1999 (26. 02. 99), 特に第0218段落及び図37参照 & EP, 874300, A & KR, 98081632, A & CN, 1202659, A	1-17, 28-44, 55-71, 82-97 18-27, 45-54, 72-81, 98-107
Y A	J P, 10-224402, A (株式会社東芝) 21. 8月. 1998 (21. 08. 98), 特に第0044段落参照, (ファミリーなし)	1-17, 28-44, 55-71, 82-97 18-27, 45-54, 72-81, 98-107

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

16. 06. 00

国際調査報告の発送日

04.07.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

丸山 高政

5W

9570

電話番号 03-3581-1101 内線 3576

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 11-27315, A (三洋電機株式会社) 29. 1月. 1999 (29. 01. 99), 特に第0003段落参照, (ファミリーなし)	3, 30, 57, 84
Y	J P, 10-21645, A (ソニー株式会社) 23. 1月. 1998 (23. 01. 98), 特に第0011~0012段落を参照, (ファミリーなし)	3, 30, 57, 84
Y	J P, 10-51439, A (松下電器産業株式会社) 20. 2月. 1998 (20. 02. 98), 特に図3参照 & E P, 809379, A & T W, 333630, A & K R, 97076418, A	6, 33, 60, 87
Y	J P, 10-210023, A (沖電気工業株式会社) 7. 8月. 1998 (07. 08. 98), 特に図2及び第0138段落参照, (ファミリーなし)	7-16, 34-43, 61-70, 88-97
A		18-27, 45-54, 72-81, 98-107
Y	Hideki Tsubakiyama and Keiichiro Koga, "Security for Information Data Broadcasting System with Conditional-Access Control," 1993 Conference Record. IEEE GLOBECOM, Vol.1, (1993), pp.164-170, 特にFig.3及びFig.4参照	9, 11, 13, 15, 17, 36, 38, 40, 42, 44, 63, 65, 67, 69, 71, 90, 92, 94, 96
A		18-27, 45-54, 72-81, 98-107
A	J P, 10-303945, A (ソニー株式会社) 13. 11月. 1998 (13. 11. 98) & E P, 874503, A & K R, 98081633, A	2-5, 29-32, 56-59, 83-86
A	J P, 10-224763, A (松下電器産業株式会社) 21. 8月. 1998 (21. 08. 98) & E P, 858183, A & K R, 98071098, A	1-5, 28-32, 55-59, 82-86
A	鈴木昌則, 藤本卓也, 影山敏宏, 北山洋幸, 小泉寿男 "映像会議シ ステム用高速シリアルバス (IEEE 1394) 通信方式" 情報処理学会研 究報告, Vol.96, No.12, (1996), pp.215-220 (96-DPS-74)	3, 4, 30, 31, 57, 58, 84, 85
A	J P, 9-74408, A (日本電信電話株式会社) 18. 3月. 1997 (18. 03. 97), (ファミリーなし)	6-27, 33-54, 60-81, 87-107
A	J P, 7-264668, A (国際電信電話株式会社) 13. 10月. 1995 (13. 10. 95) & E P, 673178, A & U S, 5596641, A	7-16, 18-27, 34-43, 45-54, 61-70, 72-81, 88-107